Technická univerzita v Liberci

Hospodářská fakulta

DIPLOMOVÁ PRÁCE

2008 Petra Vašátková

Technická univerzita v Liberci

Hospodářská fakulta

Studijní program: 6209 - Systémové inženýrství a informatika

Studijní obor: Podnikatelská informatika

Etika v prostředí Internetu

(The Internet Ethics)

DP-MI-KIN-2008-15

PETRA VAŠÁTKOVÁ

Vedoucí práce: Ing. Klára Antlová, Ph.D., Katedra informatiky

Konzultant: Mgr. Karel Severa, Katedra práva

Počet stran: 84 **Počet příloh: 7**

Datum odevzdání: 4. 1. 2008

Zadání

Prohlášení

Byla jsem seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracovala samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

Datum: 4. 1. 2008

Podpis:

Poděkování

Touto cestu bych chtěla poděkovat paní Ing. Kláře Antlové, Ph.D. za vedení mé diplomové práce.

Resumé

Diplomová práce „Etika v prostředí Internetu“ pojednává o etickém a neetickém chování uživatelů v tomto virtuálním prostředí. Po úvodu a obecné charakteristice Internetu poskytuje komplexní pohled na tuto problematiku. Nejdříve je analyzováno etické chování na Internetu, tedy pravidla chování, která by měl každý uživatel v ideálním případě dodržovat. Existuje mnoho zásad etického chování. Ty internetové sice nejsou uzákoněny, ale jsou všeobecně uznávané. Nejdříve jsou vypsány obecné zásady, které vymysleli sami uživatelé, potom pravidla chování platná pro používání konkrétní oblasti Internetu (elektronická pošta, diskusní skupiny a elektronické konference, služba WWW, služba FTP).

Práce dále pokračuje výčtem sedmnácti neetických problémů, které mohou uživatele na Internetu ohrožovat. Problémy jsou rozděleny do čtyř oblastí lidských hodnot, které mohou být neetickým chováním ohroženy. Jsou to: soukromí, vlastnictví, svoboda, morálka. Ke každému ze sedmnácti neetických problémů jsou poté nalezena řešení, jak jim čelit, popř. se jim vyhnout, včetně platné české legislativy, která uživatele také chrání. Dále je řešena pravděpodobnost a nebezpečnost jednotlivých neetických internetových problémů. Závěr obsahuje pár trendů v oblasti etiky, neetiky a ochrany proti neetickému chování.

Summary

The thesis “The Internet Ethics” deals ethical and unethical behavior of users in this virtual space. First of all there are introduction and common Internet characteristics. A general view of this topic comes after. At first the ethical behavior in Internet is analyzed. It is about the rules of behavior that should be kept by Internet users ideally. There are a lot of ethic standards used in the world. They are not legalizated, but they are generally accomplished. There are both common rules of the Internet ethics conceived by Internet users and rules for particular Internet areas (electronic mail, discussion groups and electronic conferences, WWW and FTP services) in this work.

This thesis continues with specification of seventeen unethical problems that can threaten Internet users. The problems are divided into four groups. These groups represent human values that could be damaged by unethical behavior of other users. The values are: privacy, property, freedom and morale. It was founded a few solutions for every unethical problem in the following part of the thesis. There are both preventive and defensive solutions. The Czech legislative makes another important part up that can shelter Internet user from unethical (often even criminal) behavior. Probability and dangerousness of every problem is there solved too. The end of the work contains a few trends in the area of ethics, unethics and protection against unethical behavior.

Klíčová slova

Etické chování na Internetu (netika)

Neetické chování na Internetu

Etické normy a pravidla chování

Soukromí

Vlastnictví

Svoboda

Morálka

Neoprávněné vniknutí

Špionáž

Falšování a podvody

Porušení vlastnických práv

Škodlivý software

Spamování

Cenzura

Problematický obsah webových stránek

Nepravdivé informace

Změna identity

Neoprávněná registrace doménového jména

Keywords

Ethical behavior in Internet (netiquette)

Unethical behavior in Internet

Ethical standards and behavior rules

Privacy

Property

Freedom

Morale

Unauthorized access

Spying

Counterfeiting and frauds

Proprietorial rights breaking

Harmful software

Spamming

Censorship

Problematic content of websites

False information

Identity change

Incompetent registration of domain name

Obsah

Seznam použitých zkratek a symbolů

ARPANET	Advanced Research Project Agency Network. Předchůdce Internetu. Americký armádní projekt, který se koncem 60. let minulého století snažil vzájemně spojit počítače a servery bez existence centrálního řídícího centra.
B2B	Business to business. Obchodování mezi firmami.
B2C	Business to customer. Obchodování mezi firmou a zákazníkem.
©	Copyright. Značí ochranu autorským právem.
C2C	Customer to customer. Obchodování mezi fyzickými osobami.
CDA	Communication Decency Act. Zákon USA z roku 1995, jehož snahou byla regulace obsahu webových stránek. Kvůli podezření na cenzuru byl zrušen.
DNS	Domain Name System. Hierarchický systém doménových jmen.
DSA	Digital Signature Algorithm. Šifrovací algoritmus s asymetrickým šifrováním.
DSBL	Distributed Sender Blackhole List. Veřejný seznam IP adres šířících spam.
FAQ	Frequently Asked Questions. Často kladené dotazy.
FTP	File Transfer Protocol. Služba přenosu dat mezi počítači.
IP adresa	Internet Protocol Address. Jednoznačná identifikace počítače v prostředí Internetu.
MD2, MD5	Algoritmy hashovacích funkcí.
MLM	Multi-Level Marketing. Forma obchodování.
P2P	Peer-to-peer. Architektura počítačové sítě.
PGP	Pretty Good Privacy. Program umožňující šifrování a el. podepisování.
RBL	Real Time Blocklist. Veřejný seznam IP adres, které šíří spam.
RFC	Request for Comments. Standardy popisující internetové protokoly, systémy atd.
RSA	Rivest, Shamir, Adleman. Šifra s veřejným klíčem.
SPF	Sender Policy Framework. Protokol pro popis poštovních serverů.
SSL	Secure Sockets Layer. Vrstva bezpečnostních socketů. Vrstva protokolu vložená mezi transportní a aplikační vrstvu, která pomáhá zabezpečit (šifrováním a autentizací) komunikaci mezi dvěma uživateli.
TCP/IP	Transmission Control Protocol/Internet Protocol. Sada protokolů pro komunikaci v počítačové síti.
URL	Uniform Resource Locator. Speciální název webové stránky.
WWW	World Wide Web; web. Způsob přenosu textu, obrázků, zvuku a videa na Internetu. Je členěn do webových stránek

1. Úvod

Internet je obrovská počítačová síť, která zpočátku sloužila jen malému okruhu tvůrců a uživatelů, kteří se vzájemně znali. V dnešní době je tomu však již jinak. Internetová síť dnes slouží miliónům lidí z celého světa různých národností, věku, náboženského vyznání či jiného přesvědčení ke komunikaci, zábavě, k pracovním účelům či hledání informací. Nepřekonatelná výhoda Internetu spočívá v tom, že v obrovském kybernetickém prostoru shromažďuje dosavadní lidské poznání a tím překonává klasické soubory informací, jako jsou archivy, knihovny, databáze apod.

S růstem kapacity Internetu a počtem jeho uživatelů však také rostou rizika, se kterými se uživatel může setkat. Tato diplomová práce se zabývá „správným“ a „nesprávným“ chováním uživatelů na internetové síti, jednoduše řečeno etikou na Internetu, které se zkráceně říká netiketa.

Morální zásady i právní normy se průběžně porušují i na Internetu, tak jako v každém jiném prostředí. Páchají se zde nové druhy zločinů, které jsou výzvou pro zákonodárce a jiné státní i mezinárodní orgány (Interpol). Pachatele chrání anonymita a nedostatek odpovídající legislativy, která by postihla tyto druhy přestupků a trestných činů.

Internet byl vytvořen k tomu, aby sloužil a pomáhal lidem. Lidé, kteří s Internetem pracují, často podléhají pocitům nekonečné svobody, protože si myslí, že zde neplatí žádná pravidla. Ale to samozřejmě není pravda. Podobně jako by si člověk nedovolil některé věci v reálném životě, nesmí si je dovolit ani na Internetu. Je nutné nezapomenout na slušné vychování. Ovšem uživatelé si uvědomují nutnost etického vystupování na Internetu jen pomalu.

K hlavním zásadám vypracování této diplomové práce patří komplexní pohled na etické a neetické chování uživatelů na Internetu. Po obecné charakteristice Internetu se bude věnovat obecným zásadám správného působení uživatelů v prostředí Internetu, dále pak zásadám etického chování v konkrétních oblastech Internetu (elektronická pošta, diskuse a elektronické konference, služba FTP a služba WWW).

Tato práce se dále zabývá současným neetickým chováním na Internetu a problémy, se kterými se internetová etika musí vyrovnávat. Dělí se do čtyř oblastí lidských hodnot (soukromí, vlastnictví, svoboda, morálka), které mohou být díky neetické, někdy dokonce až kriminální činnosti jiných uživatelů na Internetu narušeny. Jednotlivé hrozby budou vyjmenovány a popsány.

Ke každé hrozbě se nabízí soubor řešení, jak se má uživatel bránit, aby na něm daná nepovolená a neetická činnost nebyla páchána (preventivní opatření), dále jak se má chovat, byl-li na něm takový čin již spáchán a vše je zastřešeno právními normami, které se daným problémem zabývají, a které mohou uživatele chránit.

Také je důležité se zabývat společenskou nebezpečností všech zmíněných hrozeb a pravděpodobností, že jimi bude uživatel napaden. Jsem připravena vycházet mj. i z vlastních zkušeností a ze zkušeností mých známých a i neznámých lidí, se kterými jsem tuto problematiku probírala v internetových diskusních skupinách.

Hlavním cílem této práce je poskytnout uživateli celkový přehled jednak pravidel etického chování, dle kterých by se měli uživatelé v ideálním případě řídit, a jednak potenciálních hrozeb, s nimiž se může na Internetu setkat a způsoby, jak se těmto hrozbám a problémům vyhnout, ať už se jedná o morální poklesky či dokonce o porušování zákona a trestnou činnost. Čtenáři by měla nabídnout řadu preventivních opatření zabraňujících tomu, aby se uživatel stal obětí neetického chování. Dále pak poskytnout návody, jak minimalizovat újmy, ke kterým dochází při porušení zásad slušného chování nečestnými uživateli Internetu a nabídnout mu rady, jak se sám chovat na Internetu eticky.

Mezi dílčí cíle diplomové práce patří snaha rozlišit, které neetické činnosti se na Internetu dějí opravdu často (a na které by si měl dát uživatel dobrý pozor) od těch, které jsou pouze zveličené a přikrášlené sdělovacími prostředky. Dále si kladu za cíl rozlišit opravdu nebezpečné kriminální činy, které při používání Internetu uživateli hrozí, od těch méně nebezpečných, až po ty „pouze“ nemorální, nad kterými lze mávnout rukou.

Východiskem pro tuto diplomovou práci je můj vlastní zájem o tuto problematiku. Budu se snažit pomocí různých zdrojů sjednotit názory týkající se správného chování na Internetu v kontrastu se stále se rozvíjející internetovou kriminalitou (ať už do počtu případů, tak do stále nových způsobů, jak prostřednictvím Internetu někoho napadnout či někomu ublížit). Domnívám se, že se jedná o velice aktuální téma. Nelze přehlížet špatné stránky Internetu, ať už jde jen o neškodné žertíky, nebo o nebezpečné podvody. S Internetem souvisí i rizika, a tato práce by měla být jejich přehledem a pokusem o řešení.

2. Charakteristika Internetu

Internet je počítačová a telekomunikační síť s různým technickým a programovým vybavením. Jedná se rovněž o soubor síťových protokolů uzpůsobený k tomu, aby jednotlivé sítě mohly mezi sebou spolupracovat. Internet, nazývaný také jako síť sítí, se neřídí z jednoho centra nebo v jednom centru, ale z mnoha zdrojů. Všechny sítě spolupracující v Internetu jsou si rovny.

Internet vznikl v roce 1969 jako experimentální síť pro americkou armádu. Tato síť byla vytvořena z důvodu strachu z jaderné války. Představitelé americké armády si uvědomovali, že v případě propuknutí války by byla jako první likvidována významná centra. Proto právě v USA vznikla myšlenka vytvořit takovou komunikační strukturu, která by neměla žádná ústředí či řídící centra. Podstatou amerického armádního projektu ARPANET (Advanced Research Project Agency Network) z konce 60. let bylo spojení prostřednictvím vzájemně propojených uzlových přestupů (počítačů a serverů) tak, aby v případě válečného konfliktu při poškození či zničení jednoho z nich zůstaly ostatní ve vzájemném kontaktu. Byla prosazena speciální strategie přenosu dat na základě protokolu TCP/IP, která umožňuje komunikaci prostřednictvím různých typů komunikačních médií (telefonních linek, optických kabelů, kabelové televize, satelitů apod.) a počítačů různých typů a konfigurací.

Na konci 80. let Internet vstoupil na světovou scénu. V průběhu 90. let se začal měnit na mohutnou mezinárodní síť a jeho tempo rozvoje stále výrazně roste. Každý rok přibývá možností a funkcí Internetu, který nahrazuje stále více lidských aktivit: vyhledávání záznamů v knihovnách a katalozích, vyhledávání textů a obrazů nejrůznějších publikací, telefonování, poštovní styk, organizování skupinových setkání (porad, konferencí apod.), publikování, obchodování, nakupování, objednávání služeb, rozličné druhy zábavy atd. Internet všechny tyto a další činnosti vykonává racionálněji, efektivněji a v kratším čase, ovšem za jistou cenu, kterou může být například narušení soukromí, porušování svobody, ztráta majetku nebo poškození osobnosti.

3. Obecné zásady etiky v Internetu

Etika v nějaké oblasti lidské činnosti vždy znamená systém morálních principů a pravidel chování odvozených od všeobecných etických principů. Jedná se o tzv. etické kodexy.

V prostředí Internetu se mluví o tzv. pravidlech síťové etikety (netikety, angl. netiquette). Nejedná se o zákony, ale o všeobecně uznávané principy, přestože nepokrývají ani všechny problematické činnosti.

Etické problémy spojené s používáním Internetu se objevují postupně. S každým pokrokem v oblasti Internetu se objevují nové příležitosti, které mohou být někým zneužity. Je to částečně způsobeno velkým rozvojem Internetu, technologií s ním spojených a počtem uživatelů, který roste geometrickou řadou, jakožto i počtem oblastí, do kterých Internet začíná pronikat.

Existují pokusy sestavit nějaký obecný etický kodex pro uživatele Internetu. Dají se rozlišit dva proudy vzniku etických pravidel:

1. Pravidla organizací pro přístup a používání Internetu.
2. Zásady vznikající neformálně mezi uživateli (např. v diskusních skupinách).

3.1. Etické normy vydávané organizacemi a firmami

Jedná se o soubory norem komerčních i nekomerčních (školy, knihovny) organizací. Tyto zásady jsou mimo jiné založeny i na zákazech různých aktivit, jako jsou komerční využívání, reklama či politická propaganda.

Do komerčních organizací lze zahrnout poskytovatele připojení k Internetu a firmy, které využívají připojení k Internetu a zároveň ho poskytují svým zaměstnancům. Poskytovatelé Internetu se odkazují na obecné normy netikety. Firmy pak vycházejí ze zásad daných poskytovateli Internetu (např. využívání Internetu pouze pro pracovní účely). Uživatelé v organizaci jsou povinni se seznámit se zásadami, které stanoví jejich zaměstnavatel.

3.2. Etické normy vytvořené uživateli

Computer Ethics Institute ve Washingtonu formuloval tzv. „10 přikázání“ etického chování na Internetu [1]:

1. Nepoužiješ počítač, abys ublížil jiným.
2. Nebudeš zasahovat do práce druhých.
3. Nebudeš slídit a pohybovat se v souborech jiných.
4. Nebudeš používat počítač ke krádeži.
5. Nebudeš používat počítač k vytváření falešných informací.
6. Nebudeš kopírovat nebo používat software, který nebyl řádně zaplacen.
7. Nebudeš používat cizí výpočetní zdroje bez souhlasu majitele/odpovědné osoby.
8. Nebudeš krást jiným lidem jejich nápady.
9. Nebudeš zanedbávat sociální důsledky používání programů nebo systémů, které vytváříš.
10. Nebudeš zneužívat respekt získaný díky práci na počítači.

Další pravidla chování na Internetu vymezila Virginia Shea [5]:

1. **Nezapomínat, že se jedná o člověka.** Člověk se má k ostatním lidem chovat tak, jak si přeje, aby se ostatní chovali k němu. Jde o to, že komunikuje-li člověk v běžném životě s dalším člověkem, má kromě slov k dispozici i další prostředek komunikace, a to neverbální komunikaci (gesta, pohyby, výraz tváře, tón hlasu atd.). V online komunikaci ale tyto prostředky k dispozici nemá. Proto je při tomto způsobu komunikace velice snadné někoho urazit. Dotyčný vůbec nemusí pochopit např. ironický podtón textu. Nebo je jednoduché díky neosobnímu styku zapomenout, že komunikujeme také „jenom“ s člověkem, a ztratit tak zábrany ve svém chování. Počítačové sítě na jednu stranu rychle a snadno spojují lidi, kteří by se třeba nikdy nepotkali, na druhou stranu jde však o velice odtažitý způsob komunikace. Lidé se v elektronické komunikaci občas chovají neslušně, ačkoliv by se tak v práci či doma nikdy nechovali. Uživatel by si měl vždy položit otázku, zda by byl schopen totéž říci lidem tváří v tvář.
2. **Dodržovat stejné standardy chování jako v reálném životě.** V běžném životě většina lidí dodržuje zákony, zatímco v prostředí Internetu se přistižení při něčem nezákonném jeví jako nepravděpodobné. Lidé mají pocit absolutní svobody a myslí si, že není nutné dodržovat zásady slušného chování, protože se jedná „pouze“ o propojení lidí po síti. Opak je však pravdou. Etika a slušnost je zde stejně důležitá jako v reálném životě. Jako příklad lze uvést užívání sharewaru, kdy uživatel je za užívání povinen zaplatit autorovi malý poplatek. Spousta lidí však toto z pocitu anonymity nerespektuje.
3. **Vědět, kde se nacházím.** Např. respektovat různé netikety jednotlivých národů.

4. **Respektovat čas druhých.** Lidé mají v současnosti méně času než dříve; pracují na více projektech najednou apod. Uživatel by si měl být vědom, že pošle-li příspěvek do diskuse, dělá si tím nárok na čas jiných lidí, a tudíž by jeho příspěvek neměl plýtvat časem ostatních.
5. **Vybudovat si pověst.** Často jediná možnost, jak na Internetu zapůsobit na jiné, je psaný text. Proto by si člověk měl dát pozor na pravopis, srozumitelnost vyjadřování, logičnost, slovní zásobu, styl psaní apod.
6. **Držet pod kontrolou osobní hádky, tzv. flamewars.** Je to neslušné i vůči ostatním členům diskusní skupiny.
7. **Respektovat soukromí ostatních.** Nečíst cizí poštu, neprohlížet cizí soubory aj.
8. **Nezneužívat svou moc.** Jedná se o problém zneužívání vědomostí správců systémů, konzultantů, expertů. Vědět více než ostatní není důvod k nadřazování se nad ostatní. Např. správce systému nesmí číst soukromé dopisy.
9. **Být shovívavý k chybám jiných.** Každý jednou s Internetem začínal, každý občas udělá chybu. Taková situace by se měla přejít ze strany ostatních uživatelů mlčením, popřípadě ostatní mohou vhodným způsobem poradit. Poučování není na místě.

Netiketa vznikla samovolně. Ale jeden z popudů k jejímu vzniku byla potřeba existence etických zásad pro práci s Internetem na universitě Florida Atlantic University. Formou elektronické konference potom byly formulovány zásady, které se později staly základem RFC 1855 (viz další kapitolu).

3.3. RFC 1855

Autorkou dokumentu RFC 1855 je Sally Hambridge z firmy Intel Corporation. Jedná se o soubor pravidel síťové etikety (netikety). Jsou to spíše rady a doporučení, nejedná se o právní normu. Obsahuje rady pro uživatele, kteří na Internetu využívají osobní komunikace (elektronická pošta, rozhovor prostřednictvím počítače), kolektivní komunikace (diskuse, elektronické konference) a informačních služeb (WWW, FTP, telnet). Text tohoto standardu se nachází v příloze č. 1.

4. Zásady chování v konkrétních oblastech Internetu

Tato kapitola se zabývá pravidly, při jejichž dodržování se uživatel bude v různých částech Internetu chovat eticky. Jinak řečeno, uživatel se v následujících řádkách dozví, jak se má sám chovat, aby nebyl nařčen z neetického chování na Internetu.

4.1. Základní pravidla používání elektronické pošty

Pravidla používání elektronické pošty vycházejí z dokumentu RFC 1855 (příloha č. 1) [9].

- Je vhodné denně kontrolovat, zda do schránky (mailboxu) nepřišla nová pošta.
- Mazat nepotřebné zprávy a zbytečně je neschovávat.
- Snažit se uchovávat si v mailboxu jen nutné minimum zpráv.
- Zprávy, které budou potřeba i v budoucnu, uchovávat mimo mailbox, využít možností pro uložení do souboru na lokálním disku.
- Vyjadřovat se v dopisech stručně a jasně.
- Kvůli přehlednosti strukturovat text do odstavců. Doporučená délka odstavce je 15 řádků, je vhodné oddělovat odstavce prázdným řádkem.
- Citovat vždy přesně všechny zdroje a reference v souladu se zachováváním copyrightu a licenčních podmínek.
- Podepisovat dopisy. Podpis by měl zahrnovat jméno, organizaci, zařazení a elektronickou adresu. Neměl by být delší než čtyři řádky. Do podpisu je možno dát také adresu, číslo telefonu a číslo faxu.
- Důležitý je výstižný popis dopisu (subject). Subject pomáhá adresátovi s manipulací a zařazením dopisu. V situaci, kdy dopis nebude mít subject, odesílatel riskuje, že jeho zprávu přejde adresát bez povšimnutí a nebude ani přečtena. V případě odpovědi je nutné se ujistit, že subject odpovědi obsahuje „Re:“ nebo „Reply:“ doprovázený názvem originální zprávy.
- Nepoužívat při psaní dopisů jen velká písmena, text se tak špatně čte. Měla by se dodržovat běžná pravidla pro psaní velkých písmen. Velká písmena používat pro zvýraznění důležitých slov nebo pro odlišení dílčích nadpisů. Pro zesílení významu lze požít i jiné znaky, například *hvězdičky* kolem slova.
- Neposílat elektronickou poštou žádné informace důvěrného charakteru. Toto platí hlavně pro uživatelské jméno a heslo.

- Být opatrný na to, v jakém duchu se dopis píše. Není vhodné používat sarkasmy či černý humor. Elektronická pošta nemůže zprostředkovat vnitřní pocity pisatele, tudíž není možné poznat, že slova jsou myšlena ironicky. Je tak velmi snadné někoho, třeba neúmyslně, napadnout či zranit. Emoce se dají vyjádřit pomocí tzv. smilies (smajlíků). Viz přílohu č. 2.
- Dávat si pozor na to, co píšeme o jiných lidech. Elektronické dopisy se dají velmi snadno přeposlat třetím osobám (forward).
- Je velice netaktní přeposlat funkcí forward dopis, který byl původně poslán jako osobní. Je vhodné si vyžádat souhlas autora.
- Svými zprávami nikdy neobtěžovat. Toto zahrnuje zejména zasílání nevyžádaných reklamních dopisů, tzv. spamming (viz kapitolu 5.2.6.).
- Nepodílet se na dalším šíření tzv. řetězových dopisů. Ty vznikají nejčastěji jako varování před viry šířenými elektronickou poštou, návody na rychlé zbohatnutí či žádost o pomoc. Tyto dopisy zamořují poštovní schránky. Do této kategorie spadají i tzv. hoaxové zprávy (kapitola 5.2.6.).
- Být tolerantní k pravopisným či jazykovým chybám ostatních.
- Pokud uživatel odpovídá na dopis, je vhodné, aby součástí odpovědi byly jen podstatné věci. Souvisí to s problémem, že většina poštovních programů vkládá s funkcí „odpovědět“ do dopisu celou původní zprávu, na kterou se odpovídá. Je vhodné zkrátit tuto původní zprávu jen na věty, které souvisí s odpovědí.
- Anonymita Internetu svádí k tykání, avšak příjemcem pošty může být nadřízená osoba, starší člověk nebo žena, a proto je vhodnější používat vykání.

4.2. Základní pravidla chování diskutérů

Některé konference a diskuse mají relativně malý provoz, v jiných se naopak denně vystřídají stovky příspěvků či dopisů. Proto by měl každý uživatel zvážit, do kterých konferencí a diskusí se zapojí.

Pravidla pro používání diskusí a elektronických konferencí jsou velice podobná. Kromě obecných doporučení a zvyklostí, které platí pro elektronickou poštu (viz kapitolu 4.1.), je navíc vhodné se držet následujících pravidel:

- Dříve než začne uživatel do diskusí přispívat, je vhodné nějakou dobu sledovat zvyklosti a chování jiných uživatelů.

- Konkrétní diskuse a konference mohou mít svá pravidla. Je proto vhodné se s nimi seznámit. Tato pravidla jsou obvykle součástí potvrzení o přihlášení do konference nebo se nacházejí v souboru FAQ[1].
- Pokud uživatel hledá odpověď na nějaký konkrétní problém, existuje možnost, že daný problém již byl diskutován někdy dříve. Proto je vhodné nejdříve nahlédnout buď do archivu, nebo souboru FAQ.
- Zasílané zprávy do konference by měly být stručné, ale k věci.
- Zprávy s přiloženým souborem zasílat jen výjimečně. Předejde se tím zbytečnému zatížení sítě. Pokud je soubor dostupný prostřednictvím služeb WWW nebo FTP, stačí do diskuse poslat jen URL adresu.
- Před odesláním dotazu se vyplatí ještě jednou si jej po sobě přečíst a zkontrolovat, zda bude pro ostatní pochopitelný a zda je gramaticky správně.
- Být vůči ostatním účastníkům konference slušný. Konference slouží k výměně názorů a musí se počítat s tím, že se všechny nebudou shodovat.
- Pokud je posílán do konference dotaz, je lepší si nechat posílat odpovědi na svou osobní adresu a ne přes konferenci. Do konference se pak pošle jen souhrn všech příspěvků s odpověďmi s nadpisem „Shrnutí“.
- Uživatel by měl respektovat přání tazatele a poslat svůj příspěvek na adresu, kterou si přál (konference či konkrétní osoba).
- Pokud některý uživatel zašle do konference dotaz, který je mimo téma konference, pak je vhodné neodpovídat mu prostřednictvím konference, ale přímo na jeho osobní adresu.
- Po přihlášení do nové konference si uchovat potvrzení o přihlášení, které obsahuje užitečné informace (mj. i o tom, jak se z konference zase odhlásit).
- Zjistit, kam je posílána přihláška/odhláška pro konferenci. Adresa pro administrativní úkony je vždy jiná, je nevhodné obtěžovat ostatní účastníky konference.
- V případě delší nepřítomnosti, kdy uživatel nemůže vyzvedávat svou poštu, je vhodné se z konferencí odhlásit či pozastavit příjem dopisů.
- Neposílat tentýž dopis do mnoha konferencí. Mohlo by dojít k crosspostingu. Jedná se o jev, kdy uživatel několika konferencí dostane stejný dotaz několikrát, protože jiný uživatel rozeslal svůj příspěvek do více konferencí. Crossposting zbytečně zatěžuje počítačovou síť a ubírá uživatelům čas.
- Neposílat dotaz do konference, pokud jeho obsah nesouvisí s tématem konference.
- Pokud se uživatel přistihne, že zprávy z některé konference nečte, je dobré se z ní odhlásit.

[1] Frequently Asked Questions, často kladené dotazy.

4.3. Pravidla správného používání služby FTP

- Pokud je to možné, je vhodné omezit přenosy velkých souborů během běžné pracovní doby (nejen lokální, ale hlavně vzdáleného počítače). Upřednostňovat ranní nebo večerní hodiny.
- Respektovat časová omezení, která jsou na některých archivech. Brát v úvahu časová pásma, neuvažovat jen v lokálním čase.
- Uživatel musí dodržovat licenční podmínky a autorská práva u programů získaných z veřejných archivů[2]. Řada programů je pro volné užití, ale u některých je nutno zaplatit drobný poplatek. Je proto vhodné se seznámit s podmínkami zadané autorem programu.

4.4. Pravidla správného používání služby WWW

- Nikdy se nespoléhat na to, že informace získané z WWW serveru jsou pravdivé a aktuální. Důležité informace čerpat jen ze seriózních serverů, o kterých je známo, že poskytují korektní údaje.
- Při posuzování designu WWW dokumentů být tolerantní. Co se nelíbí jednomu, se může líbit druhému a naopak. Není příliš vhodné posílat autorovi WWW stránek dopis, že design není hezký. Připomínky by se měly posílat jen v případě nalezených chyb (špatně fungující odkazy, chybějící položky apod.).

[2] Různé kategorie šířených programů – Public Domain, Freeware, Shareware, Demoware, GNU General Public License (GPL) – jsou vymezeny v kapitole 6.5.1.

5. Oblasti porušování etiky v prostředí Internetu

Oblasti, ve kterých je internetová etika porušována, se dají rozdělit následovně: soukromí, vlastnictví, svoboda, morálka. V této kapitole jsou oblasti rozděleny do podkapitol, ve kterých jsou popsány prostředky a praktiky, pomocí nichž jsou tyto čtyři oblasti lidských hodnot ohrožovány.

5.1. Soukromí

Jak říká citát Janlori Goldmana[3]: „Nebezpečí Internetu spočívá v iluzi anonymity provozu.“ Uživatelé se mylně domnívají, že v prostředí Internetu pracují skryti před ostatními uživateli.

5.1.1. Hackeři a crackeři

Hacker dříve znamenal tvůrčího uživatele počítače a schopného programátora. Časem se však označení „hacker“ vžilo pro člověka, který zneužívá svých znalostí a který se chová jako počítačový pirát. Proto raději používejme pojem „cracker“.

Cracker je zákeřný člověk, který vniká do počítačů cizích lidí a narušuje tak soukromí uživatelů. Koná tak pomocí nedostatků v softwaru či hardwaru počítače, využívá chyb v bezpečnostním systému. Crackeři se dělí do několika skupin podle toho, jak moc velké nebezpečí pro uživatele představují. Někteří chtějí jen zjistit, co všechno dokážou a kam až mohou zajít, někteří crackeři však dokážou poškodit např. systém uživatele, narušit jeho soukromí či mu zničit pověst tím, že se za něj vydávají. Často dokážou pozměnit cizí WWW stránky nebo vykrást různé databáze. Nejhorší typ crackera je ten, který nabourává systém ne pro zábavu, ale pro svůj zisk a užitek.

Heslo je důležitým bezpečnostním prvkem každého systému. Heslo je v systému uloženo v zašifrovaném tvaru a ani správce počítače nemá možnost ho zjistit. Kontrola hesla se provádí tak, že se po zadání zašifruje a porovnává se se zašifrovaným heslem. Je nutné vybírat hesla tak, aby nebylo uhodnutelné případným crackerem nebo speciálním programem na uhodnutí tajných hesel.

Sociotechnika (sociální inženýrství)

Sociotechnika je ovlivňování lidí s cílem je oklamat a přesvědčit je, že sociotechnik je osoba, za kterou se skutečně vydává. Této schopnosti využívá k získání informací, které hodlá zneužít.

[3] Právník z washingtonského Střediska pro demokracii a technologii.

Jedná se o crackerskou techniku, jejímž cílem je oklamat wetware[4] tak, aby lidé prozradili svá hesla či jiné osobní informace. Druhy útoků:

- Útočník požádá oběť o uživatelské jméno a heslo.
- Útočník předstírá, že je někdo z nadřízených oběti, který má problém a potřebuje ho rychle vyřešit. Pod touto záminkou si vyžádá informace o softwaru, jeho konfiguraci, tel. číslo atd.
- Útočník předstírá, že je nový zaměstnanec, který má potíže s přihlášením do firemní sítě.
- Cracker předstírá, že je firemní informatik, a s touto identitou vyláká od uživatelů tajná data.
- Cracker zinscenuje situaci tak, aby se na něj sama oběť obrátila s prosbou o pomoc.

Hackeři a crackeři samozřejmě při své nekalé činnosti používají mnoho různých prostředků, např. různý škodlivý software, falšování zpráv apod. Viz další kapitoly.

5.1.2. Sběr osobních dat uživatelů prostřednictvím Internetu

Jeden z důvodů nedostatku soukromí na Internetu je neexistence oficiálních pravidel, která by vymezovala, které informace jsou soukromé. Protože neexistuje omezení, které by bránilo využití těchto informací třetími osobami, tak se nelze divit, že je v Internetu mnoho osobních údajů, se kterými lze volně nakládat. Často vznikají různé pochybné firmy, které se živí sbíráním osobních profilů uživatelů a jejich následným prodejem.

Dnes již běžně funguje, že monitoringem veřejně dostupných informačních zdrojů (diskusních skupin) a bezplatných vyhledávacích služeb si některé firmy zapisují e-mailové adresy uživatelů a využívají je k zasílání spamu nebo prodávají adresy dále. Kromě aktivit v konferencích a diskusních skupinách lze zjistit, které WWW servery uživatel navštěvuje nejčastěji, počítá se také s nedostatečnou zabezpečeností elektronické pošty, elektronických nákupů a plateb.

Cookies

Cookies se objevují při práci s prohlížečem WWW stránek. Cookie je textový soubor, který se ukládá na lokálním disku uživatele. Cookies sbírají pro WWW servery demografické a reklamní informace (počet návštěv stránek uživatelem, jaké konkrétní odkazy ho zajímají, jaké výrobky si zakoupil apod.). Samotné cookies nejsou nebezpečné. Cookies mohou být využity jen tím serverem, který je do počítače uživatele uložil. Záleží na WWW serveru, jak se získanými informacemi naloží, ale úmysly nemusejí být vždy čisté. Existují také způsoby, jak se k informacím jednoho severu může dostat jiný server.

[4] Lidský nervový systém.

Spyware

Spyware je skrytý program pracující v počítači uživatele, který odesílá velké množství důvěrných informací třetím osobám. Mezi informace, které je schopen spyware zjistit a odeslat, patří jméno uživatele, IP adresa, seznam programů nainstalovaných na počítači, záznamy o aktivitě uživatelů a mnoho dalších dat. K místům, kde uživatel k takovému spywaru může přijít, patří shareware a adware aplikace, výměnné sítě (P2P), WWW stránky s nelegálním a erotickým obsahem, elektronická pošta, některé FTP servery, Instant Messaging apod.

5.1.3. Porušení soukromí elektronické pošty

Mnoho uživatelů považuje komunikaci prostřednictvím elektronické pošty za důvěrnou a bezpečnou. Není to však pravda. Elektronická pošta při své cestě od odesilatele k adresátovi prochází mnoha mezistanicemi. Z toho plynou následující nebezpečí: dopis může přečíst někdo cizí, dopis může být změněn a dopis nemusí být pravý. Proto by měl uživatel svou poštu zabezpečit.

Způsoby špehování elektronické pošty [3]:

1. Při psaní elektronické zprávy může keylogger zjistit, co uživatel vyťukává na klávesnici.
2. Po odeslání zpráva pobývá v prostoru pro nahrávání uvnitř počítače. V této době si ji může správce systému přečíst.
3. Zpráva po opuštění počítače se přenáší přes řadu dalších počítačů v různých sítích, jejichž bezohlední uživatelé si ji můžou přečíst.
4. Po doručení zprávy do počítače adresáta se elektronický dopis nachází v souboru „nepřečtená pošta“, kde si zprávu může přečíst správce systému.
5. Po přihlášení adresáta a stahování elektronické zprávy na obrazovku může dopis zachytit keylogger.
6. Adresát uloží zprávu do nějakého souboru. Pokud ho nezabezpečil, může si ho kdokoliv přečíst.
7. Adresát může zprávu zálohovat. Pokud ji kdokoliv najde, může si kopii přečíst.

Existují i různé služby státu, které jsou dle příslušných zákonů[5] oprávněny elektronickou komunikaci odposlouchávat. Patří k nim např. Bezpečnostní informační služba, armáda, různé složky policie (kriminální, služba policie pro odhalování korupce a závažné hospodářské trestné činnosti, celní úřad apod.). V této souvislosti se mluví o odposlechu a záznamu telekomunikačního,

[5] Zákon o Bezpečnostní informační službě [37]; zákon o Policii České republiky [34]; trestní řád [21] – § 86, § 87, § 88 – Zadržení zásilky, Otevření zásilky, Odposlech a záznam telekomunikačního provozu.

radiokomunikačního a podobného provozu, což se vztahuje i na internetovou komunikaci. K zahájení odposlechu je třeba mít soudní příkaz. Bez příkazu lze účastníka odposlouchávat jen v případě, je-li vedeno trestní řízení a zároveň s tím účastník souhlasí.

5.1.4. Falšování elektronických zpráv, WWW stránek a příspěvků v diskusních skupinách a konferencích

V rámci soukromí a bezpečnosti elektronické pošty se často mluví o falšování různých zpráv či WWW stránek, což umožňuje člověku vydávat se za jinou osobu a odesílat poštu jeho jménem. Padělání e-mailových zpráv spočívá v rozluštění speciálního e-mailového jazyka, kterým komunikují všechny počítače připojené k Internetu. Cracker pronikne do uživatelského účtu a posílá e-maily nebo přispívá do diskusí pod jménem tohoto uživatele.

Při čtení e-mailové zprávy adresát vidí v odesilateli jinou osobu, než tu, která dopis opravdu odeslala. Někdy se může jednat o nevinný žert, ale takovýto „nepravý“ dopis může mít i vážné následky (např. rozesílání nenávistných, rasistických, pomluvných zpráv…), které někomu mohou zničit pověst. Nepoctivý uživatel si může pomocí této metody „zfalšovat“ kladná doporučení do zaměstnání.

Phishing

Phishing vzniklo ze spojení slov phreaking + fishing (česky rhybaření). Jedná se o spam s podvrženou adresou odesilatele, který směřuje uživatele na taktéž podvrženou stránku, která je připravena k tomu, aby uživatele přesvědčila k vyzrazení citlivých dat (např. týkající se internetového bankovnictví). Stránka tedy obvykle napodobuje banku nebo internetového prodejce a ukládá osobní data uživatele. Tato metoda může fungovat i na principu keyloggeru (viz kapitolu 5.2.5.) nebo prostředníků SSL[6]. Phishing je založeno na sociálním inženýrství (viz kapitolu 5.1.1.).

Pharming

Pharming je spojením slov phreaking a farming (česky farmaření). Cílem je opět získat citlivé (hlavně bankovní) údaje od uživatelů. Tentokrát se tak děje pomocí přesměrování uživatele na falešnou IP adresu podvržených webových stránek (útočí tedy na DNS[7]). Pharming je nebezpečnější než phishing, protože v tomto případě nestačí jako obrana obezřetnost a zdravý rozum.

[6] Secure Sockets Layer (vrstva bezpečnostních socketů), vrstva protokolu vložená mezi transportní a aplikační vrstvu, která pomáhá zabezpečit (šifrováním a autentizací) komunikaci mezi dvěma uživateli.
[7] Domain Name Server.

5.2. Vlastnictví

Právo na vlastnictví patří k základním lidským právům chráněných Ústavou České republiky [15]. V prostředí Internetu se ve spojitosti s vlastnictvím mluví o duševním vlastnictví, autorských právech, případně o porušování těchto práv. O svůj majetek může uživatel přijít také prostřednictvím různých internetových podvodů, působením škodlivého softwaru nebo obchodováním s nepoctivým uživatelem či firmou. Dalším problémem pro uživatele může být doručování spamu, který ho nepochybně okrádá o čas, a ten, jak je známo, znamená peníze.

5.2.1. Porušování vlastnických práv

V prostředí Internetu jsou krádeže duševního vlastnictví značně rozšířeny. Kopírovat se dá software, WWW dokumenty, diskusní příspěvky či příspěvky v elektronických konferencích. Jedná se zejména o vytváření nelegálních kopií. Pro uživatele je velice jednoduché přenést soubor či text, aniž by riskoval, že jeho počínání bude odhaleno. Mezi nejčastěji nelegálně kopírované elementy patří audiovizuální nahrávky a počítačové programy.

Je nutné dodat, že předměty, kterých se týká duševní vlastnictví, jsou intelektuálním obsahem (informací, myšlenkou, nápadem) a nikoliv formou (kniha, elektronický dokument), v jaké se prezentují na Internetu. V dnešní době existují různé instituty, které se zabývají duševním vlastnictvím a jeho ochranou. Patří mezi ně copyright (autorské právo) nebo patent.

Co se týče WWW dokumentů, existuje plagiátorství dvojího druhu. Jednak lze okopírovat obsah WWW stránky, a pak formu prezentace WWW dokumentu (hlavně design, barvu, prvky, rozmístění, nápad a myšlenka)[8].

Každý autor práce, ať už se jedná o vědeckou, semestrální či diplomovou práci, by měl uvést všechny použité prameny (včetně WWW dokumentů), ze kterých do své práce čerpal. Nesouvisí to jen s ochranou autorských práv, ale také s informační etikou. Existují tři hlavní důvody citace použitých pramenů: jednak dodržení zákona (v rámci ČR autorského zákona), získání kontextu vyhledáním originálního díla a upřesnění citovaných informací.

[8] Jako příklad lze uvést případ z roku 1997, kdy se český Internet rozrostl o nový vyhledávač katalogového typu nazývaný HotList. Z velké části šlo o kopii oblíbeného Seznamu.cz, který již měl za sebou dvouleté úspěšné fungování, a ze kterého si HotList odnesl jak obsah (říkalo se, že dokonce včetně překlepů a chyb), tak i celkový design. HotList se od Seznamu odlišoval jen v maličkostech. Plagiátorství bylo tak zřejmé, že sami tvůrci Seznamu vyvinuli nátlak na tvůrce HotListu, aby své stránky stáhli. Do týdne se Seznamu stažení stránek podařilo prosadit.

Omyly uživatelů týkající se ochrany autorských práv [1]:

1. Není-li v materiálu uvedena poznámka o copyrightu, pak tento materiál není chráněn copyrightem.
2. Materiál je veřejně a zdarma dostupný, proto jej mohu volně použít.
3. Materiál byl zaslán do elektronické konference, proto má charakter public domain[9].
4. Měl jsem čisté úmysly.
5. Jestliže nechráníte svou práci pomocí copyrightu, pak na něj ztrácíte nárok.
6. Vytvořím-li svou práci na základě jiných děl, pak práva přísluší mně.
7. Autor mi poslal elektronickou poštou kopii, proto ji mohu volně použít.

Nejčastější způsoby porušování autorských práv na Internetu [2]:

- Přivlastňování si (spolu)autorství cizího díla.
- Neuvedení nebo nepřesné uvedení autora.
- Zásah do díla (např. programu, WWW stránek) bez souhlasu autora.
- Použití díla bez souhlasu autora (okopírování, prodej kopií).
- Nezaplacení autorské odměny za užití díla.

Jak již bylo řečeno, mezi nejčastější případy porušování autorského práva na Internetu patří softwarové pirátství, dále pak porušování autorských práv u hudby a filmů. Hudební nahrávky bývají zkomprimovány, odeslány a přenášeny po celém světě prostřednictvím Internetu bez placení těm, kdo do tvorby investovali. V poslední době se stále více rozmáhá neoprávněné sdílení filmových souborů prostřednictvím Internetu. Často jsou nelegálně sdílené soubory umístěny na internetových serverech vzdělávacích institucí.

Potrestán musí být jednak ten, kdo programy pirátsky šíří, a jednak ten, kdo je používá. Počítačové pirátství hřeší na globálnost Internetu, nejasnosti, které vznikají při právním určení, kde se skutek stal a jaká země ho má vyšetřovat, a problémem je také spolupráce s některými zeměmi světa.

Dle „Výroční studie BSA-IDC o softwarovém pirátství ve světě“ míra softwarového pirátství v České republice klesá a v současné době se pohybuje okolo 40%, čímž se Česká republika řadí mezi 20 zemí světa s nejnižší mírou softwarového pirátství.

[9] Viz kapitola 6.5.1.

5.2.2. Scamy a podvodníci slibující rychlé zbohatnutí

Scamy a různé podvody se stále rozrůstají, protože tzv. scammerům (podvodníkům) nahrává několik skutečností. Například to, že mohou skrýt svou osobu pod pseudonym, a tím pádem jsou téměř nevystopovatelní. Scammeři využívají nezkušených uživatelů. Další výhodou pro scammery je, že šíření scamů po Internetu je téměř zdarma. Návody „jak rychle zbohatnout" se objevují ve všech médiích již od jejich vzniku a Internet není výjimkou. Následuje několik známých druhů.

Pyramidová schémata neboli letadla

Pyramidová schémata nabízejí rychle vydělané peníze. Spočívají ve vytváření seznamů adres a v jejich prodeji. Obecný princip spočívá v tom, že 1 osoba pošle určitý obnos několika lidem, každý z nich pošle peníze dalším několika lidem, z nichž každý z nich pošle peníze dalším pár lidem atd. Následující tabulka znázorňuje zisk z pyramidy se vstupním poplatkem 20 Kč a 5 osobami získaných každým dalším účastníkem.

5 osob	5 * 20 Kč	100 Kč
1. generace	25 * 20 Kč	500 Kč
2. generace	125 * 20 Kč	2 500 Kč
3. generace	625 * 20 Kč	12 500 Kč
4. generace	3 125 * 20 Kč	62 500 Kč
5. generace	15 625 * 20 Kč	312 500 Kč
Zisk		**390 600 Kč**

Tab. 1: Znázornění zisku z pyramidové hry; zdroj: [3, str. 60].

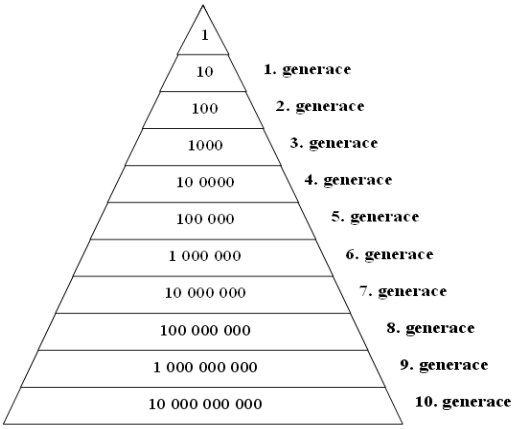
Jeden ze způsobů fungování „pyramidy" na Internetu popisuje následující případ. Přijde e-mail, ve kterém jsou uvedena jména a adresy 10 lidí. Příjemce e-mailu musí poslat prvním pěti lidem ze seznamu např. 50 korun. Potom vyškrtne ze seznamu první jméno a přidá své na konec seznamu. Na závěr musí elektronický dopis poslat deseti dalším lidem. Při rozšiřování dopisu jméno přidaného uživatele šplhá po seznamu nahoru, až se objeví mezi prvními pěti. A pak by měly začít chodit tisíce padesátikorunových částek. Účastníci v každé generaci pyramidy posílají peníze těm, kteří jsou nad nimi, a získávají peníze od těch, kteří stojí v pyramidě pod nimi. Toto je však jenom teorie, v praxi se pyramida nefunguje a jedná se o podvod. Někteří lidé se dají na tento princip nalákat, protože tvůrci pyramid dobře ovládají psychologii skupin.

Důvody, proč pyramida nefunguje:

1. Když by se uživatel dostal na začátek seznamu (i v případě poslušného posílání vždy 10 dopisů každou generací dalším 10 lidem), bylo by ve hře 9 generací lidí, kteří odeslali dopisy. To znamená asi 1 miliarda lidí (viz obr. 1). V dalším kole by bylo ve hře 10 mld.

osob, což je mnohem více, než je počet obyvatel zeměkoule. Kdyby pyramida opravdu fungovala, museli by se jí zúčastnit a zbohatnout všichni lidé na světě. Což nejde, protože peníze by se neměly v pokročilých generacích odkud čerpat.

2. Spousta lidí takovéto výzvy v dopisech ignoruje a řetěz poruší. Tím pádem se šance na „výdělek“ násobně snižuje.



Obr. 1: Nárůst počtu lidí zapojených do pyramidy s každou další generací hry; zdroj: vlastní.

Zisk z toho mají jen scammeři, protože nehrají podle pravidel pyramidy. Neposílají pár, ale tisíce dopisů, což jim Internet umožňuje s minimálními náklady. Jiný způsob výdělku: scammeři vyberou vstupní poplatky a pak se vytratí a nechají pyramidu postupně vymizet. Pyramida je nezákonná, protože slibuje lidem peníze, které má šanci dostat jen podvodník, a to autor pyramidy.

Ponzi schémata

Ponzi schémata fungují podobně jako pyramidová schémata. Podvodník zaplatí slíbené „výdělky“ jen prvním investujícím. Scammer získá dobrou pověst. Počet účastníků se rozšiřuje, vyplacení účastníci peníze znovu investují, ale jednoho dne podvodník i s penězi zmizí.

Velké výdělky za několik dní

Značně rozšířeny jsou inzeráty slibující velké výdělky za krátkou dobu, většinou při práci doma (vystřihování z novin, slepování hraček, vybarvování dřevěných kalendářů apod.). Firmy po pracovníkovi většinou chtějí, aby si zakoupil vybavení, které potřebuje k práci. Chce to aktivní přístup člověka, rychlou práci, nebo si člověk nevydělá ani na vložené náklady. Firmy poté chtějí, aby lidé výrobky (po kterých je malá poptávka) sami prodávali. Celý podvod je založen na tom, že firmy mají zájem pouze na tom, aby prodali počáteční materiál a vybavení lidem, kteří z nich mají něco vyrábět.

5.2.3. Podvody v nabízení zboží, služby

Dalším problémem, se kterým se uživatelé Internetu musí vyrovnávat, jsou inzeráty prodávající (i použité) zboží za mnohem vyšší cenu než se dá pořídit nové v kamenném obchodě. Jedná se většinou o zboží, které běžný člověk nekupuje každý den, a tudíž nemá přehled o ceně. Pokud jsou uživateli na Internetu nabízeny nějaké kupóny či slevy, měl by být opatrný. Je možné, že i po uplatnění slevy se nákup zboží nevyplatí. Nebo je možné, že si firma naúčtuje neúměrně vysoké poštovné a balné.

Podvody prostřednictvím tajného zástupce

- Některé firmy využívají tajného zástupce do diskusních fór a recenzních stránek k propagaci svého zboží, kde takový „recenzent" velice kladně hodnotí firemní výrobky.
- Na zpravodajských serverech se objevuje inzerce, která vypadá jako novinový článek, ale jedná se o skrytou reklamu.
- Firmy uveřejňující své inzeráty, vydávající se za běžného uživatele. Jedná se o další skrytou reklamu – vypadá jako uživatel, který prodává nějakou věc, pronajímá nemovitost (ve skutečnosti realitní kancelář), nabízí „svůj" zájezd (ve skutečnosti cestovní kancelář).
- Některé firmy předstírají, že uživatele znají a navedou ho např. na firemní webové stránky.
- Ankety, které slouží ke komerčním účelům nebo ke sběru dat odpovídajících.
- Rozesílání e-mailů, které „jsou určeny někomu jinému", a které upozorňují na nějaký produkt, službu, firmu či její WWW stránky.

„Hledači talentů"

Existují osoby, které tvrdí, že pomůžou lidem stát se slavnými. Například tvrdí, že pracují pro hollywoodskou filmovou společnost a hledají nové talenty. Nebo slibují, že vydají CD začínajícím a zatím neobjeveným hudebním skupinám a zpěvákům. Často jsou inzeráty na takové služby doplněny výroky typu: „Bereme všechny!" nebo „Ukažte celému světu svůj talent!", což je samo o sobě nesmysl. Podvod spočívá v tom, že inkasují tisíce poplatků od důvěřivých lidí bez jakékoliv poskytnuté protislužby.

Návody

Za poplatek také scammeři slibují různé návody, např. jak se vyhnout placení daní, poštovného apod. Ale buď jejich návody nefungují, či uživatel po zaplacení poplatku žádný návod ani nedostane. V nejhorším případě tyto návody stojí mimo zákon a uživateli hrozí vězení za daňové úniky či poštovní podvody. Podvodníci pouze chtějí prodat své návody a nestarají se o to, že mohou někoho dostat do vězení.

5.2.4. Prodej běžně dostupných informací

Existují lidé, kteří se snaží prodat nějaké informace, které lze získat jinde a zdarma. Za poplatek tak uživatel obdrží různé „tajné“ rady a návody jak ušetřit, které jsou však zřejmé i bez návodu či běžně dostupné jinde. Takové inzeráty nabízejí informace o tom, jak ušetřit nebo vydělat peníze, zbavit se dluhů nebo být úspěšný. Takové informace jsou prezentovány jako tajné nebo obtížně dostupné. Jedná se např. o aukce, seznamy velkoobchodníků či seznamy lidí, se kterými si uživatel může dopisovat.

5.2.5. Škodlivý software

Malware vznikl složením slov malicious (záludný) + software. Jedná se o počítačový program, který slouží k vniknutí či poškození počítačového systému. Do malware můžeme zařadit počítačové viry, trojské koně, spyware (viz kapitolu 5.1.2.) a adware.

Mezi nejrozšířenější hrozby pro počítačové systémy uživatelů patří viry a červi. **Počítačové viry** jsou části počítačového kódu, který se připojí k programu či souboru tak, aby se mohl šířit z počítače do počítače a infikovat je. Jedná se o trestnou činnost, která vzniká okamžikem, kdy se virem infikuje počítač někoho jiného. Nelegální je již příprava takového viru, ovšem u této skutečnosti se těžko prokazuje, že pachatel připravoval nějaký útok. Škody na majetku uživatele, které viry páchají, jsou následující:

- Náklady na odstranění viru.
- Náklady na kontrolu, opravu nebo obnovení poškozených dat z archivních kopií.
- Náklady na opětovnou instalaci poškozených programů.
- Náklady na znovuvytvoření poškozených (nezálohovaných, nearchivovaných) dat.
- Nepřímé škody (náklady na nákup a provoz antivirového softwaru) apod.

Červi jsou stejně jako viry určené k tomu, aby se kopírovali z počítače do počítače, ale činí tak automaticky přebíráním kontroly nad funkcemi počítače. Velkým nebezpečím červů je jejich schopnost nekontrolovaně se množit. Červi umí například odeslat kopie sebe samého komukoliv, kdo je uveden v adresáři kontaktů, a jejich počítače pak mohou učinit to samé, což způsobí dominový efekt a velmi vysoké provozní zatížení na síti. Základní filozofií červa je získat určitý stupeň kontroly nad strojem, do kterého se dostal, dále se prostřednictvím sítě rozmnožovat a vykonávat nějakou činnost.

Trojský kůň, stejně jako ten mytologický, přináší „dary“, který by uživatel rozhodně za „zdmi“ svého počítače nerad viděl – narušují jeho bezpečnost a mohou způsobit mnoho škod. Je to program, který může obsahovat vir, nechtěnou funkci, o níž uživatel neví, nebo na ni nebyl předem upozorněn.

Adware přidává do nainstalovaných programů (jedná se většinou o freewarové či sharewarové programy) reklamu. Jsou to komponenty programu, které slouží k zobrazování reklamního proužku nebo pop-up okna s reklamou. Pokud program nevyžaduje připojení na Internet, aby mohl stáhnout další reklamní proužky nebo tajně na pozadí odesílat informace, je jeho činnost neškodná. Pokud tomu tak není, stává se **spywarem** (v kapitole 5.1.2.).

Dialer je program, který dokáže změnit způsob přístupu na Internet. Místo běžně používaných čísel pro internetové připojení přesměruje vytáčení na čísla s často výrazně vyšší tarifikací.

Keylogger je software, který dokáže zaznamenat stisknutí jednotlivých kláves na klávesnici, klikání myší na ikony, dále dokáže sejmout obrazovku či zaznamenat seznam navštívených stránek. Antivirový program ho považuje za virus. Jedná se o jakousi formu spyware.

5.2.6. Spamming

Spam je nevyžádaná pošta. Jde o reklamní e-mail, kterým se spammeři zahlcují schránky uživatelů. Spamování je považováno za trestný čin, přesto množství zaslaných e-mailů tohoto charakteru stále vzrůstá. Spamming je založen na principu posílání jedné kopie nevyžádané zprávy více příjemcům současně.

Spamování neboli spamming je nelegální aktivita, v rámci které původce spamu (spammer) obtěžuje příjemce nevyžádané pošty a nutí je svým počínáním vynakládat čas, pozornost a úsilí na aktivity (rozpoznávání spamu a jeho rušení), které by za normálních okolností nevykonávali. Příjemce navíc hradí větší část nákladů na tyto aktivity (přenos nevyžádaných zásilek – buď přenosový čas, nebo objem přenesených dat), ačkoliv s tím nesouhlasí. Spam je nebezpečný právě z důvodu zahlcení kapacity e-mailové schránky, které může vést k neobdržení důležitého e-mailu. Navíc může být např. nositelem virů nebo trojských koní.

Spamming se týká nejen elektronické pošty, ale i chatů, diskusních fór a elektronických konferencí. Za spam se považuje i rozesílání neslušných, provokativních, urážlivých či výhružných zpráv, zpráv vyzývajících k nesnášenlivosti (rasové, náboženské i jiné), či zpráv, které se jinak neslučují

s pravidly všeobecné lidské slušnosti (viz kapitolu 5.4.1. Neslušné chování na Internetu). [2] Každý uživatel má právo na to, aby nebyl při práci, vzdělávání nebo i hraní na Internetu rušen.

Se spamem souvisí i tzv. **hoax** a hoaxové (žertovné, podvodné) zprávy. Jedná se o zprávu, která se šíří mezi uživateli a obvykle obsahuje falešný poplach, před něčím varuje, žádá o pomoc, nebo se snaží pobavit a zároveň žádá příjemce, aby zprávu odeslal dále. Nejenže je rozesílání takových zpráv neetické, ale může dokonce příjemce obtěžovat, nabízet nebezpečné rady atd.

Dalším nebezpečným a nepříjemným jevem, který se šíří pomocí elektronické pošty, je **mailbombing**, neboli bombardování zprávami. Zde nejde o obsah zprávy, ale o to, že chce-li někdo uživateli uškodit, pošle mu velké množství (třeba i těch samých) zpráv, čímž mu zcela zahltí e-mailovou schránku.

5.2.7. Nástrahy obchodování po Internetu

Elektronický obchod je obchodem, při kterém komunikace mezi jeho účastníky probíhá zčásti nebo zcela po standardních počítačových sítích, prostřednictvím počítačů, jejich příslušenství a telekomunikací. (technická interpretace) [2]

Elektronický obchod lze také definovat jako přenos projevu vůle související s jednáním o určitém obchodu, respektive uzavřením obchodní smlouvy, který je zčásti nebo zcela přenášen prostřednictvím počítačových sítí respektive počítačů propojených komunikacemi. (právní interpretace) [2]

Internetové obchodování funguje následujícím způsobem: Zákazník si vybere podle popisu, fotografie či jiného druhu prezentace na webových stránkách zboží, které požaduje. Nebo mu je zboží nabídnuto. Dále následuje objednávka zboží a ověření totožnosti kupujícího prodávajícím. Prodávající by měl být dostatečně ztotožněn na webových stránkách. Pak by mělo dojít k výměně zboží či služby za peníze. Záleží na druhu obchodu, zda bude nejdříve provedena úhrada, doručena prodávajícímu a pak teprve dodáno zboží, či nejdříve posláno zboží (např. na dobírku) a poté kupujícím uhrazena peněžní částka.

Existují různé stupně obchodování po Internetu. Jednou variantou je marketing výrobku, výběr, objednání zboží, veškerá komunikace i platba – vše prostřednictvím Internetu. Druhou variantou je, že kupující si na webových stránkách (nebo např. i v tištěném médiu) vybere zboží a elektronicky pouze objedná zboží (prostřednictvím e-mailu) u prodejce. K spoustě obchodních transakcí (např.

s použitým zbožím) dochází i pomocí podaných inzerátů na inzertních serverech. Obchodovat mezi sebou mohou jednak společnosti (B2B)[10], jednak fyzické osoby (C2C), a pak i společnosti s fyzickými osobami (B2C).

Spousta uživatelů využívá výhod obchodování po Internetu. Obchodování po Síti je rychlé, snadné, většinou levnější, nabízí se rozmanitější zboží, obrovské množství potenciálních kupců a prodejců. Každý většinou na Internetu najde kupce pro své byť i neobvyklé zboží. Většina obchodníků je poctivá, někteří ale ne. Příčin nefunkčnosti této cesty nákupu a prodeje je několik: nedorozumění, zpoždění e-mailů, podvody. Při obchodování na Internetu je nejdůležitější dbát co nejvyšší bezpečnosti. Když ale uživatel obchoduje po Internetu s někým, koho nezná, nikdy nelze zajistit úplnou bezpečnost transakce. Přesto by lidé neměli na nakupování po Síti zanevírat. Výhody této cesty obchodování jsou nesporné, a pokud bude uživatel znát různé druhy pastí a používat zásady bezpečnosti, může rizika snížit na minimum.

Pravděpodobnost, že se uživatel stane obětí podvodníka, je velmi malá. Lidé však mají vysoký pocit ohrožení. Souvisí to s tím, že je-li uživatel s transakcí spokojen, nikdo se o tom nedozví. Zažije-li však nějakou nepříjemnou zkušenost, určitě se ozve. Tudíž je vždy slyšet jen ty nespokojené uživatele a lidé získají dojem, že se nejedná o dostatečně bezpečný obchodní kanál.

5.3. Svoboda

Obecně svoboda znamená schopnost i možnost volit, rozhodovat a jednat podle svého, a zároveň jednat také odpovědně. Slovo svoboda může být použito v několika významech, ať už máme na mysli náboženskou svobodu, svobodu projevu či např. shromažďovací svobodu. Celkově vzato je „svoboda“ pro jednotlivce maximální, omezená pouze svobodou jiného jedince.

Z hlediska etiky rozlišujeme svobodu rozhodování a svobodu jednání.

Svoboda rozhodování znamená míru vnitřní svobody člověka rozhodovat se mezi alternativami. V tomto smyslu Internet působí pozitivně na svobodu rozhodování, protože podporuje snadnější a rychlejší přístup k velkému množství informací. Lidé potom mohou být informovanější, a tím i svobodnější při svém rozhodování. Naopak se jedinci může stát, že se stane na Internetu závislým, a tím se omezí jeho vnitřní svoboda rozhodování.

[10] B2B – business to business; C2C – customer to customer; B2C – business to customer.

Svoboda jednání potom znamená, jak moc je jednání jedince omezeno vnějšími okolnostmi. Se svobodou jednání souvisí anonymita. Anonymita znamená, že člověk může svobodně jednat bez možnosti, aby ho někdo odhalil jako původce jednání. Konkrétně se jedná především o využívání elektronické pošty nebo služeb skupinové komunikace (konference, diskusní skupiny).

5.3.1. Cenzura a regulace obsahu WWW stránek

Cenzura neboli omezování svobody tvorby s sebou přináší omezení volného publikování nějaké informace. Nejde však o omezování publikování vědecké nebo umělecké práce, ale souvisí s problémem narůstání materiálu na Internetu s problematickým charakterem (pornografie, násilí, terorismus, sekty apod.). Řešením tohoto problému by se mohla stát cenzura nevhodných WWW stránek. Cenzura se však zdá sama o sobě problémem.

V České republice je cenzura v jakékoliv formě zakázána, a tudíž s tímto nemáme zkušenosti. Ve Spojených státech však zkoušeli jakousi regulaci obsahu WWW stránek zavést, a to zákonem Communication Decency Act of 1995 (CDA), neboli zákon o kontrole obsahu dokumentů v prostředí Internetu, který byl dodatkem návrhu zákona o telekomunikacích.

Platnost tohoto dodatku však neměla dlouhého trvání, a to právě z důvodu podezření na cenzuru a porušování svobody slova. Zákon byl tedy prohlášen za protiústavní a zrušen.

CDA obsahoval návrh, že obscénní, pornografický, lascivní, sprostý či nemravný materiál by byl na Internetu a službách online postaven mimo zákon, pokud by k nim měly přístup nezletilé děti [3]. Porušit tento zákon mohli jak uživatelé, tak poskytovatelé Internetu a tresty za porušení byly až 100 000 dolarů a odnětí svobody až na dva roky.

Lidé, kteří nesouhlasí s cenzurou Internetu, jsou obviňováni, že podporují dětskou pornografii a jiné ohavnosti. Cenzura na Internetu nebude nikdy úplně fungovat. Objem informací je obrovský a uživatelé, kteří si myslí, že jejich svoboda projevu je ohrožena, by určitě našli způsob, jak obejít zákazy, které na ně uvalí nějaký zákon. Internet je schopen se velmi rychle přizpůsobovat.

5.4. Morálka

Neetické chování popsané v této kapitole nemůže uživatele nějak vážně ohrozit na majetku, svobodě či soukromí. Může ho však v tom lepším případě pohoršit nebo zesměšnit, v tom horším případě mu zničit pověst. Problémy popsané v této kapitole tedy nejsou o nic méně vážné než třeba útok crackera či spamming.

5.4.1. Neslušné chování na Internetu

Často se neslušné chování uživatelů Internetu projeví v diskusních skupinách a konferencích. Problémem některých diskutujících je, že jim nezáleží ani tak na vyjádření svého názoru, jako na tom někoho urazit, zesměšnit nebo se chovat jinak nevhodně, často s použitím vulgarit. Někteří lidé se diskusí neúčastní, aby diskutovali, ale aby se hádali. Částečně se na tom podílí fakt, že účastníci se přihlašují do diskusí pouze pod přezdívkami, tzv. nicky, a tudíž se s pocitem dokonalé anonymity dopouští neetického chování.

Flamer je účastník flamewar, který agresivně hájí své názory. **Flamewars**[11] mohou být zábavné i otravné. Ale probíhají-li takové války a vášnivé výměny názorů v rámci nějaké diskusní skupiny, ostatním uživatelům může vadit, že než se dostanou k informacím, které potřebují, musí se prokousávat nadávkami a urážkami. Navíc připojí-li se uživatel do takové války, stojí ho to značné množství času.

Troll je účastník diskuse, který se snaží někoho zesměšnit, vyvolat hádku či rozvrátit diskusi, přičemž se nestydí používat očividně chybné hlášky a vulgarity. Troll je také internetová zpráva, jejímž cílem je přimět lidi, aby na ni odpověděli, a tak je dostat do nepříjemností. Lidé vytvářející trolly nutí uživatele, aby na jejich nesmyslné výroky odpovídali, a tím je zdržují a také zesměšní. Troll vytvoří nějaký nesmyslný příspěvek v diskusi, a pak zmizí a přihlíží jen jako divák, popřípadě dalšími příspěvky rozdmýchává diskusi a velice se tím baví. Záleží mu na emocionálních příspěvcích, které ostatní pobuřují. Na nesmyslný nebo pobuřující článek trolla lze reagovat následovně: Buď článek ignorovat, napsat dopis autorovi nebo odpovědět a připojit se k diskusi. V posledním případě se uživatel nechal trollem nachytat. Podlehne-li uživatel nutkání ozvat se na příspěvek trolla, stane se akorát terčem posměchu.

Trollování či flamewars můžou probíhat jak v diskusních skupinách, tak i chatech nebo prostřednictvím elektronické pošty.

[11] Ohnivá diskuse, plamenná válka, slovní potyčka na Internetu.

Křivá obvinění, urážky na cti, pomluvy, diskreditace[12]

Člověk při výše uvedených aktivitách podstupuje riziko, že bude obviněn, že poškozuje něčí pověst a dopustí se křivého obvinění. Křivé obvinění v písemné podobě se nazývá urážka na cti. Na Internetu uživatel může někoho urazit, protože máme svobodu slova, ale nesmí ho křivě obvinit. Urážka na cti musí splňovat tyto body:

- Musí to být lež.
- Výrok musí být hanlivě vyjádřen; tak, aby mohl poškodit pověst člověka.
- Musí být oznámeno třetí straně (např. ostatním chatujícím na chatu).
- Musí být psána se škodolibým úmyslem.

K dalším nevhodným a trestným činům na Internetu patří **vyhrožování**, **vydírání** a **obtěžování**.

5.4.2. Prezentace nevhodného nebo nebezpečného obsahu na stránkách Internetu

Do nevhodného a nebezpečného obsahu WWW stránek se mj. řadí:

- násilí,
- dětská pornografie, propagace pedofilie, zoofilie,
- návody na výroby výbušnin,
- obchodování se zbraněmi,
- navádění k trestné činnosti a terorismu, schvalování zločinnosti,
- propagace nacismu,
- sekty,
- další extremistické projevy (neonacismus, ultraradikální komunismus, českofašismus, extrémní nacionalismus apod.),
- propagace nesnášenlivosti,
- myšlenky napadající lidská a občanská práva,
- organizování mafií,
- šíření toxikomanie,
- vše, co ohrožuje mravnost a vývoj mládeže atd.

Po celém Internetu existují stovky otřesných videí a oblázků poprav, mučení, lidských nehod atd. Návštěvnost takových webových stránek je obrovská, jde hlavně o muže. V důsledku sledování těchto materiálů se z člověka může stát cynik či dokonce v něm zažehnout podobné chování.

[12] Podrytí něčí důvěry nebo důvěryhodnosti.

Chování vyznačující se vyhledáváním těchto materiálů může být považováno za perverzní. Na jednu stranu, odolným jedincům lze ukázat cokoliv a jejich chování to neovlivní, nestanou se z nich kriminálníci ani devianti. Na druhou stranu, když už někdo perverzní sklony má, pohled na brutální záběry ho může podnítit k trestnému činu. Tyto činy však v dotyčném již dřímají. Internet by tedy neměl být přímo příčinou, nýbrž spouštěčem takového patologického chování.

Od historičtějších případů prezentace násilí, jako jsou popravy a mučení na veřejnosti nebo gladiátorské hry, se Internet liší pouze tím, že tuto podívanou lze šířit masově, je lehce dostupná a vyznačuje se poněkud větším odstupem od reality. Na druhou stranu existuje názor, že některé úchylky, jako je například pedofilie, může pomoci Internet zneškodňovat (tím, že dotyčný se spokojí s materiálem z Internetu a neobtěžuje své oběti v reálném životě). Pravda o tom, jaký vliv má Internet na devianty, je někde mezi těmito dvěma názory. [8]

Přístup dětí k problematickému obsahu na WWW stránkách

Nevhodné a nebezpečné informace na WWW stránkách mohou ublížit hlavně dětem, které neumí tak dobře rozlišovat mezi dobrem a zlem, jako dospělí. Existují příběhy dětí, které naletěly pedofilům, které si denně prohlíží erotické materiály nebo se účastní debatních skupin, kde se otevřeně diskutuje o sexu. Je pravda, že takové případy se určitě stávají, ale novináři, kteří o takových věcech velmi rádi píší, aby vyvolali senzaci, velmi často věc nafukují do obrovských rozměrů, protože ve skutečnosti se jedná o případy velice vzácné a neliší se od míry nebezpečí, kterému musí děti čelit v reálném světě.

Ve skutečnosti problém erotiky na Internetu, ke které mají přístup děti, je zveličený a existuje v této oblasti spoustu mýtů. Není pravda, že děti jsou vystaveny erotice na Internetu proti své vůli. Takový materiál si musejí ve většině případů vyhledat. Dalším mýtem je skutečnost, že velké množství elektronických zpráv obsahuje pornografické obrázky. Spoustu lidí si také myslí, že díky Internetu bylo uneseno nebo pronásledováno mnoho dětí. Ve srovnání s množstvím únosů, které nemají s Internetem nic společného, se jedná o zanedbatelnou část. Dalším problémem jsou eroticky podbarvená slova, která se však na Internetu objevují ve stejné míře, jako v ostatních médiích.

5.4.3. Prezentace nepravdivých a zavádějících informací na Internetu

Na Internetu se objevuje velké množství informací, jejichž pravdivost nemůže být nikdy zaručena. Své webové stránky si totiž může vytvořit kdokoliv a vložit tam cokoliv se mu zlíbí. Názory, zkušenosti a cíle jednotlivých uživatelů Internetu se různí – a tudíž se různí i jejich „pravdy“.

A žádná opravdová kontrola přesnosti informací neexistuje. Pokud si uživatel vybere nepravdivý zdroj, riskuje, že udělá špatné rozhodnutí, zaujme nesprávný postoj nebo udělá špatný závěr.

Žertíky, novinářské kachny, fámy, spekulace, legendy a pověsti

Pokud se uživatel u takového žertíku či novinářské kachny baví, nelze to brát jako vážný problém nebo ztrátu času. Pokud ho však různé praktiky a legrácky jiných uživatelů stojí námahu, peníze nebo vyvolají nedůvěru, jedná se o vážnější situaci. Občas takové jednání hraničí s neetickým jednáním, ale uživatele nijak neohrozí. Problém nastane, vezme-li někdo takový žert vážně a uvěří mu. Ztratí tak spoustu času a může ho to i před ostatními znemožnit. Dále mohou být promarněny prostředky při hledání skutečnosti. Pokud nějaká spekulace či vymyšlená zpráva vyvolá mezi uživateli obavy či strach, může se dokonce jednat o šíření poplašné zprávy.

Google bombing

Google bomba zneužívá vlastností internetového vyhledávače (nejčastěji Google). Útok funguje na principu zadání nějakého slova či fráze, kdy vyhledávač nevyhledá jen WWW stránky obsahující řetězec znaků, ale odkazuje i na stránky osob či skupiny osob s kritickým nebo humorným úmyslem, často s politickým podtextem. Zneužitelná je funkce vyhledávače, kdy po zadání hesla „XY“ se vypíší i takové webové stránky, aniž by obsahovaly slova „XY“, protože stránky se obsahově se k zadanému heslu hodí (popisují ji tak lidé, kteří vytvořili odkaz na hledanou stránku a nazvali ho „XY“). Tato funkce má sloužit ke zkvalitnění vyhledávací služby, ale je velice snadno zneužitelná. Vytvoří se spousta odkazů na určité WWW stránky, odkazy se přitom hanlivě nebo urážlivě nazvou, a už se jedná o Google bombu. Čím více odkazů se vytvoří, tím je větší šance, že se cílová stránka ocitne při vyhledávání na prvním místě, což je cílem Google bomby.

Mezi časté cíle Google bomb patří v České republice osobní stránky českých politiků a stránky politických stran. Např. v roce 2004 po zadání hesla „Velký bratr“ Google zobrazil stránky Stanislava Grosse, v roce 2006 se po zadání hesla „namyšlený ješita“ objevily stránky Jiřího Paroubka, heslo „zločinci a vrazi“ zase zobrazilo stránky politické strany KSČM. Ze zahraničí lze uvést heslo „miserable failure“ (mizerné selhání), které zobrazilo odkaz na stránky amerického prezidenta George W. Bushe.

5.4.4. Změna identity

Díky Internetu mohou lidé rychle, levně a anonymně komunikovat s desítkami či stovkami lidí z celého světa. Po nějaké době komunikace po Internetu[13] může uživatel získat dojem, že dotyčné lidi zná. Že poznal jejich zájmy, jejich touhy, povahu či smysl pro humor. Opak je však pravdou.

Internetová vs. skutečná osobnost člověka

Je nutné rozlišovat skutečnou a internetovou osobnost člověka. Mohou být stejné, ale také se mohou velice lišit. Ostatním mohou prezentovat jiný věk, rasu, vzhled i pohlaví, než jakým disponují. Lidé se na Internetu často dělají jinými, než jsou. Je to neškodné a většinou na tom nezáleží, ovšem do té doby, než dojde k osobnímu setkání, které může přinést velké zklamání. Často se také stává, že dva lidé, kteří si dopisují a rozumí si po Internetu, si ve skutečnosti při živém setkání vůbec nesednou. Anonymita Internetu totiž zanechává při komunikaci mezery ve znalostech internetových přátel a mozek si tyto znalosti sám doplní[14]. Nelze poznat člověka jen podle toho, co o sobě píše. Někteří lidé to nedělají záměrně, pouze o sobě tvrdí, co si o sobě myslí, i když to nemusí být pravda.

Změna identity kvůli bezpečnosti

V dnešní době se zdá, že jednou z hlavních zásad chatování i jiné komunikace na Internetu je „hlavně nešířit pravdivé údaje“. Jedná se o takovou hru, na kterou chatující přistupují, a o které se veřejně ví. Chatující lidé ze strachu, aby se nedostali do nějakého problému, zamlčují nejen své pohlaví, ale i věk, vzdělání aj. Zároveň přehánějí a předstírají snad všechno, co se předstírat dá.

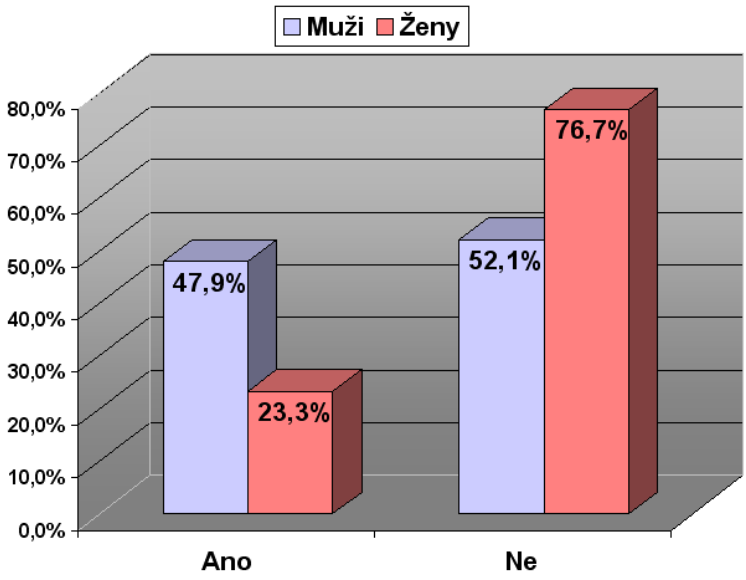
Říká se, že v takových prostředích jako je chat a různé druhy seznamek a diskusí se s přetvářkou a falešností počítá. Všichni návštěvníci vstupují do místností pod přezdívkou (tzv. nickem), protože prozradit o sobě takové informace jako jméno, příjmení a adresu je občas velký hazard. Skutečné informace tedy uživatelé neprozrazují už z důvodu ochrany vlastního soukromí.

Výhody změny identity

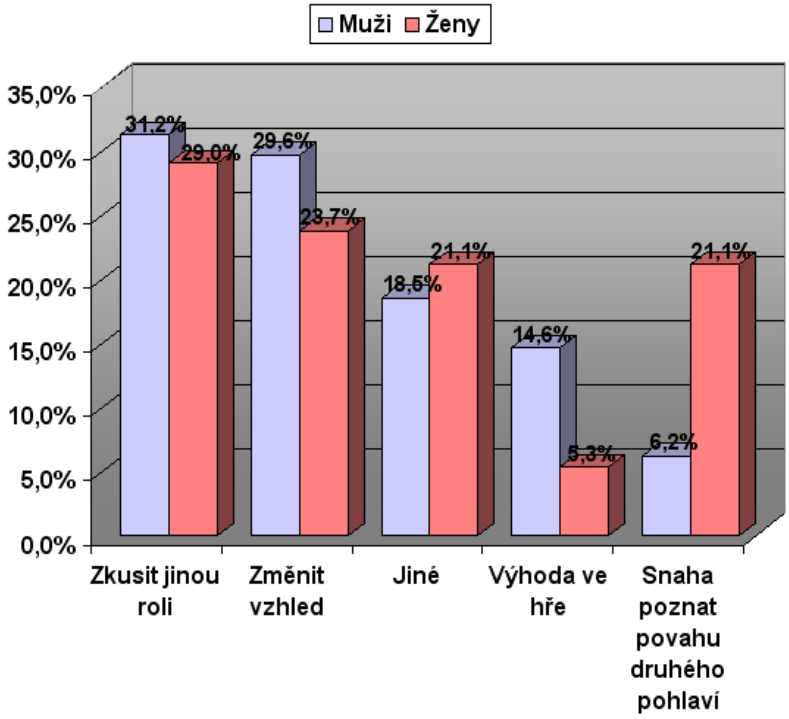
Nikdo se pod rouškou anonymity nestydí vyslovit svůj vlastní, třeba i neobvyklý názor a ani si nedělá starosti, zda jeho způsob komunikace je či není slušný. Jedná tak v domnění, že se mu nic nemůže stát. Na druhou stranu bez uzardění lže a zkouší, kam až může zajít. Je sice pravda, že v poslední době o takové nezávazné debaty opadá zájem a lidé raději vyhledávají na Internetu specializované diskuse na konkrétní témata. V takovém „vážnějším“ prostředí už jsou uživatelé

[13] Chatování, diskutování ve skupinách, komunikování prostřednictvím elektronické pošty.
[14] Sigmund Freud tomuto jevu říkal transference.

ochotni na sebe prozradit více. Na druhou stranu existují přímo i fantasy chaty, kde se uživatel přímo stylizuje do nějaké fiktivní postavy.



Graf 1: Změnili jste alespoň jednou na Internetu pohlaví?; zdroj: The Daedalus Project, 2007.



Graf 2: Důvod změny pohlaví na Internetu; zdroj: The Daedalus Project, 2007.

Většina lidí chodí na chat se bavit a nezávazně si promluvit, a třeba si i vyzkoušet nějakou jinou sociální roli, což nemusí být na škodu, pokud se tak neděje pořád. Uživatelé musí umět rozlišit virtuální svět od toho skutečného a vědět, že ne vše, co se nachází na Internetu, musí být pravda. Taková změna identity je tedy dobrá k tomu, že lidé jsou k sobě absolutně upřímní, a tudíž mohou zjistit, zda se k sobě hodí. Změnu své identity například používají lidé, kteří hledají na Internetu partnera. Existují i lidé (např. homosexuálové), kteří mění svou identitu ze strachu před nadávkami, ne z potřeby někoho podvádět.

Změnu identity spousta lidí používá jen pro zábavu, ale jsou i tací, kteří tímto způsobem získávají od ostatních lidí důvěru a obírají je o důvěrné informace, o peníze nebo se chovají nezodpovědně.

Existují dva názory na tento přístup [12]. Dle psychologů se jedná o povrchní zábavu a nevhodný způsob, jak trávit svůj čas. Tvrdí, že se jedná o prostředí plné na první pohled možná zajímavých informací, ale pravdivých prý těžko. A i kdyby pravdivé byly, uživatel o tom nikdy nezíská úplnou jistotu. Na druhém názoru trvají lidé, kteří chatují (chataři), kteří povrchnost naopak vytýkají odborníkům, kteří je kritizují. Obviňují je z arogantního chování, aniž by zjistili, jak chatování funguje.

5.4.5. Neoprávněná registrace doménového jména

Právo k přidělení doménového jména v určitém tvaru má ten, kdo si zažádá dříve. Známé jsou podvody, kdy si vychytralí uživatelé koupili doménové jméno s názvem nějaké firmy, instituce či známé osobnosti (celebrita, politik), a které se následně snažili prodat tomu, komu jméno patří, samozřejmě za mnohem větší sumu. V horším případě si pod tímto doménovým jménem vytvořili stránky s nepravdivým či pobuřujícím obsahem. Nebo takovéto doménové jméno zneužila konkurence firmy.

Cybersquatting znamená ukradení názvu atraktivní domény. Porušuje hospodářskou soutěž, např. vůči názvům měst, krajů, obcí apod. Jedná se o poškozování cizích práv. V případě, že se za její přenechání někomu jinému požaduje úhrada, může se jednat i o trestný čin vydírání.

6. Ochrana proti neetickému chování na Internetu

Tato kapitola pojednává o možnostech ochrany proti neetickému (neslušnému, nevhodnému a občas až kriminálnímu) chování ze strany ostatních uživatelů. Jednak navrhuje preventivní opatření, kterými může uživatel eliminovat útoky na svou osobu, a pak obsahuje návody, jak se chovat v situacích, kdy se k němu jiný uživatel chová neeticky či dokonce byl nějak napaden.

Každá podkapitola, která představuje vždy nějaký problém neetiky řešený na Internetu, obsahuje rady a prostředky pro preventivní a bezpečné chování na Internetu a obranu před zmiňovaným problémem.

Tato práce se mj. zabývá i českým právem v oblasti Internetu. Všeobecný zákon, který by vymezoval, jak by se měli uživatelé chovat na Internetu, zatím neexistuje. Existují ale některé zákony, vyhlášky a směrnice, které se týkají mj. také Internetu, a řeší některé otázky jako je ochrana autorských práv na Internetu, nelegálnost rozesílání spamu a nevyžádané pošty, dále zda patří e-mailová adresa do osobních dat, jejichž prodej je nelegální, nebo zda lze design webové stránky označit za autorské dílo, na něž se vztahuje zákaz kopírování. Každá podkapitola obsahuje tedy i zákony, které k problému Internetu patří a které mohou pomoci v řešení situace.

6.1. Průnik hackerů a crackerů do cizího počítače

6.1.1. Bezpečnostní pravidlo: Bezpečí při velkém počtu [3]

Toto pravidlo vychází ze skutečnosti, že při tak velkém množství uživatelů v síti Internet je pravděpodobnost napadení crackerem velmi malá. Na druhou stranu je třeba říci, že se zvyšující se výkonností počítačů je tato zásada méně účinná, protože cracker zvládne prohledat a napadnout více uživatelských počítačů najednou. Dále by uživatel neměl šířit, že na jeho počítači se nachází tajná data a tím na sebe upozorňovat.

6.1.2. Bezpečnostní pravidlo: Bezpečí díky neznalosti [3]

Toto pravidlo vychází z toho, že na obsluhu obtížný software nemůžou zneužít „obyčejní“ uživatelé. Je nutné mít v tomto ohledu speciální vzdělání. Z toho vyplývá, že málokdo má potenciál na zneužití softwaru. Je nutno dodat, že čím je Internet rozšířenější, roste vzdělání v tomto oboru, a stále více uživatelů je schopno prolomit bezpečnost nějakého systému.

6.1.3. Ochrana dobrým heslem

Je nutné, aby si uživatel vytvořit důmyslná hesla, která případný vetřelec neuhodne a i programy na uhodnutí tajných hesel budou mít menší či žádnou šanci na uhodnutí.

Špatná hesla [11]:

- Jméno, příjmení, přezdívka.
- Jméno nebo příjmení příbuzných.
- Rodné číslo, číslo občanského průkazu, číslo pasu.
- Oblíbené jídlo, značka auta, hudební skupina, kniha.
- Cokoli, co o uživateli mohou vědět kolegové nebo jiní lidé.
- Křestní jména a slova ze slovníků.
- Znaky ležící vedle sebe na klávesnici.
- Cokoliv z výše uvedeného doplněné o jednu číslici.
- Cokoliv z výše uvedeného pozpátku.
- Příliš krátká.
- Veřejně známá „vhodná hesla“.
- Heslo napsané na klávesnici nebo v kalendáři vedle počítače.

Dobrá hesla [11]:

- Minimálně 6 znaků dlouhé.
- Obsahuje malá i velká písmena.
- Obsahuje číslice a speciální symboly.
- Vymyšlené slovo, spojení dvou nesouvisejících slov, proložená slova (lichá písmena z jednoho, sudá písmena z druhého slova), první písmena z věty v knize či písni (ne uživatelovi oblíbené). Vše s vloženými číslicemi a speciálními znaky, některá písmena velká.

V žádném případě hesla nezveřejňovat! Heslo by se mělo uchovat v tajnosti, tzn. nikomu se neříkat, nikam ho nezapisovat, nedat se podvodnými taktikami přesvědčit k jeho vyzrazení.

6.1.4. Pozor na sociotechniku a jiné triky

- Cracker sleduje, co uživatel píše na klávesnici při zadávání hesla.
- Falešný e-mail od správce systému (viz problematiku sociotechniky v kapitole 5.1.1.), kdy
    - žádá o prozrazení hesla nebo
    - žádá o změnu hesla na heslo, které určí apod.

- Nepoužívat raději účty jiných osob. Uživatel si může vypůjčit účet od jiné osoby – crackera. Cracker dříve vytvořil „falešný program“, do kterého se podvedený uživatel přihlásí zadáním svého jména a hesla. „Falešný program“ si pak jméno i heslo pamatuje. Připomíná tzv. phishing nebo pharming (kapitola 5.1.4.). Při práci na veřejných počítačích by měl uživatel před začátkem práce počítač restartovat.

Není dobré triky crackerů tajit. Někdo může namítat, že zveřejní-li se takové triky a návody, naučí se je více uživatelů, kteří je budou provádět také. Ale ve skutečnosti je lepší o nich veřejnost informovat, aby si uživatelé dali pozor, protože v dnešní době se již tolik nelze spoléhat na „bezpečnost díky neznalosti“ (viz kapitolu 5.1.2.).

6.1.5. Programy pro hádání hesel

Tyto programy může cracker použít, aby zjistil uživatelské heslo. Může je však použít sám uživatel, aby zjistil, zda jeho heslo vyhovuje a není uhodnutelné. Příklady programů: BRUTUS AET2, EMAIL CRACK, WWW HACK, GoldenEye apod.

6.1.6. Neodcházet od počítače po nalogování

Platí to pro veřejné internetové kavárny, také pro kancelář, kde uživatel pracuje se svými kolegy nebo školní učebnu, kterou student sdílí se svými spolužáky. Crackerovi stačí pár vteřin na vytvoření chyby v bezpečnostním systému nebo změně hesla k programu, a pak už se dostane na účet kdykoliv. Není nutné se odhlašovat vždy při odchodu od počítače. Existují tzv. blokovací (lock) programy, které po spuštění zablokují klávesnici a myš pomocí hesla. K odblokování je potřeba zase jen heslo. Lze také použít šetřiče obrazovky, po jejichž spuštění se lze do systému dostat zase jenom po ověření heslem.

6.1.7. Přístupová práva k souborům

Pokud je to v systému uživatele možné, uživatel by si měl přístupová oprávnění k souborům nastavit. Zabrání tak tomu, aby se k jeho dokumentům dostali cizí lidé.

6.1.8. Šifrování důležitých souborů

Šifrování znamená transformaci souboru do nesrozumitelného tvaru, do nahodilé směsice znaků, a k dešifrování je potřeba heslo. K šifrování dat na disku se používá symetrická varianta, kdy

uživatel svá data chrání jediným heslem, s jehož pomocí data šifruje i dešifruje. Mezi nejčastěji používané symetrické šifry patří AES, Blowfish, 3DES nebo Serpent. Více v kapitole 6.3.1.

6.1.9. Legislativa

Trestní zákon [20]

Dle § 257a odst. 1: Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užije,
b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.[15]

V případě, že se cracker dostane do cizího počítače a jenom si data prohlíží (nemaže, nemění ani nekrade), nedošlo k naplnění § 257a odst. 1 písmena a) a b), ale určitě došlo k naplnění písmena c). Dle § 152[16] při hackerské činnosti dochází také k porušování ***autorského zákona***.

6.2. Sběr osobních dat prostřednictvím Internetu

6.2.1. Chránit své osobní údaje

Mezi důvěrná data, která lze uchránit, můžeme považovat skutečné jméno uživatele, jeho adresu a telefon. Stačí, když tyto údaje zná jen správce systému. Heslo uživatele pak nezná ani správce. Dále lze chránit soubory na počítači, informaci o výši majetku uživatele (včetně informace o vybavení vlastního počítače v diskusních skupinách) atd. Uživatel může chránit i svůj počítač, tzn. alespoň se nevzdalovat od počítače po nalogování. Uživatel musí striktně rozlišovat mezi veřejnými a tajnými informacemi a podle toho se chovat.

---

[15] § 257a trestního zákona [20]:
(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.
(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

[16] (1) Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

6.2.2. Použití anonymizérů a remailerů

Uživatel si může vyžádat anonymní adresu na počítačové službě anonymní remailer. Tato služba umožňuje účastnit se diskusí a dalších aktivit s anonymní zpáteční adresou. Poštovní remailery umožňují přijímat a odesílat zprávy anonymně. Jedná se o systém, který využívá směrování a neprolomitelného šifrování. Při používání nevznikají záznamy o jejich činnosti nebo se hned ničí. Všechna tato opatření vedou k tomu, že ani samotní správci remailovacích serverů nedokážou nic zjistit o odesilatelích, příjemcích a dokonce ani obsahu zprávy.

Výhody těchto remailerů, mezi které nepochybně patří ochrana osobních dat uživatele, jsou vyváženy jejich nevýhodami, a to možností jejich zneužití při páchání neetické či trestné činnosti (spamming, prezentace nebezpečných informací apod.) Spousta remailerů je k dohledání na WWW adrese:

http://www.theargon.com/achilles/remailer/

Webové anonymizéry fungují podobně jako e-mailové remailery; umožňují skrýt identitu při prohlížení WWW stránek. Některé anonymizéry:

http://www.anonymizer.com/
http://www.anonymizer.ru/
http://anonymouse.ws/
http://www.the-cloak.com/anonymous-surfing-home.html
http://www.anonymization.net/
http://www.proxyweb.net/
http://webwarper.net/ww?info=1
http://www.2gm.cz/?page_id=10
http://anonymizer.secuser.com/

6.2.3. Boj se spywarem

Základem je pravidelné používání programu na detekování a ničení spywaru (tzv. antispyware). Mezi nejpoužívanější programy patří:

Spybot – Search & Destroy (uživatelské rozhraní viz přílohu č. 4)
Spyware Terminator
Ad-Aware SE Personal Edition (uživatelské rozhraní viz přílohu č. 3)
AVG Anti-Spyware Free
Spy Sweeper

Dále se vyplatí používat firewall (viz kapitolu 6.9.), neprohlížet podezřelé WWW stránky, používat bezpečný internetový prohlížeč, neinstalovat podezřelé programy a pravidelně aktualizovat svůj operační systém. Zneužití cookies lze zabránit např. pomocí programu Ad-Aware, který cookies nalezne a vymaže nebo lze v prohlížeči cookies zakázat.

6.2.4. Legislativa

Listina základních práv a svobod [15]
Článek 7, odstavec 1: Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Zákon o ochraně osobních dat v informačních systémech [33], který byl prvním zákonem, který definoval informatické pojmy a stanovil základní pravidla týkající se nakládání s osobními údaji. Vychází z Listiny základních práv a svobod a doporučení Rady Evropy a Evropských společenství. V době svého přijetí byl však již zastaralý, nedokonalý a neobsahoval sankce.

Zákon o ochraně osobních údajů [27]
Od jeho přijetí v roce 2000 byl již několikrát novelizován. Vymezuje, co je myšleno pojmem osobní údaje a jak se s nimi může zacházet. Vztahuje se na státní orgány, obchodní společnosti, provozovatele serverů a poskytovatele služeb na Internetu. Nevztahuje se na zpracování osobních údajů fyzickými osobami.

Zákon vymezuje pojem osobní údaj, čímž myslí každý údaj, který se týká určeného nebo určitelného subjektu údajů, což znamená situaci, kdy lze na základě jednoho či více osobních údajů zjistit identitu subjektu.

Zákon chrání fyzické osoby, ne osoby právnické. O osobních údajích lze hovořit pouze ve spojení s fyzickou osobou. Správce může osobní údaje zpracovávat pouze se souhlasem subjektu, kterého se údaje týkají. Souhlas může být odvolán.

Problémem je získávání osobních údajů uživatelů za účelem jejich dalšího marketingového využití. Znamená to např., že prodejce získá jméno a adresu (i e-mailovou) zákazníka při prodeji zboží, a tuto adresu použije dále např. k rozesílání reklam, nabízení jiného zboží apod. Spamming tohoto druhu lze provozovat pouze do té doby, než to zákazník zakáže. Podobným problémem je, když banka poskytne osobní údaje klientů partnerské spořitelně. V tomto případě je hranice slušnosti již překročena.

Dle § 5 tohoto zákona může správce, který zpracovává osobní údaje, předat tyto údaje jinému správci pouze za těchto podmínek:

- údaje subjektu údajů byly získány v souvislosti s činností správce nebo se jedná o zveřejněné osobní údaje,
- údaje budou využívány pouze za účelem nabízení obchodu a služeb,
- subjekt údajů byl o tomto postupu správce předem informován a nevyslovil s tímto postupem nesouhlas (myšleno písemně).

Z novely tohoto zákona vyplývá, že stačí, když uživatel jednou sdělí spammerovi, že si nepřeje dostávat jeho nabídky, a ten by se měl postarat o to, aby uživatel již nebyl obtěžován.

Jednou z nejdůležitějších povinností správce je shromažďovat osobní údaje pouze k tomu účelu, k němuž byly shromažďovány (výjimku tvoří policejní a daňové účely). Správce (např. provozovatel e-shopu) je povinen co nejdříve každou osobu informovat o tom, že o ní shromažďuje údaje, v jakém rozsahu, proč, kdo a jak je bude zpracovávat a jakým způsobem budou zveřejněny. Pokud správci neposkytnul osobní údaje přímo uživatel, je povinen uživateli sdělit, odkud údaje získal (zdroj osobních údajů).

Podmínky pro zpracovávání tzv. citlivých údajů[17] jsou následující:

a) souhlas subjektu údajů (výslovný, písemný a podepsaný), je odvolatelný, může být nahrazen zvláštním zákonem[18],
b) zájem na ochraně jeho života, zdraví či jiných důležitých hodnot,
c) pokud tak stanoví zákon.

V prostředí Internetu je nemyslitelné, aby osobní údaje byly zasílány mezi aplikacemi nešifrovaně. Pokud někdo s těmito údaji pracuje, je nutné, aby provedl audit bezpečnosti svého informačního a komunikačního systému, zavedl vhodná bezpečnostní opatření a tím minimalizoval možnost vlastního trestního postihu. Sankce za porušení zákona o ochraně osobních údajů mohou být až do výše 50 000 Kč pro fyzické osoby a 20 000 000 Kč pro správce. Existují i další zákony chránící osobní data uživatelů[19].

[17] Osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údaje.
[18] Zákon o Policii České republiky [34]; zákon o zpravodajských službách České republiky [35].
[19] Zákon o bankách [36]; zákon o ochraně utajovaných skutečností [39].

Trestní zákon [20]

Dle § 178 – Neoprávněné nakládání s osobními údaji – ten, kdo i z nedbalosti neoprávněné sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem. Pokud jsou údaje vyzrazeny prostřednictvím sdělovacích prostředků (včetně WWW stránek), způsobí subjektu údajů vážnou újmu, nebo tak učiní porušením povinností ve svém zaměstnání, může být potrestán odnětím svobody až na 5 let.

Neoprávněným nakládáním s osobními údaji může být poškozena pověst, rodinný život či způsobeny problémy v zaměstnání osoby, které se údaje týkají.

V Internetu jsou od uživatelů běžně sbírána data, aniž by k tomu měli provozovatelé systémů oprávnění, a aniž by to uživatelé věděli. Často za to však mohou sami uživatelé, kteří sdělí své důvěrné údaje, aby např. získali nějakou službu. Dojde-li však k jejich zneužití správcem, existují pro něj různé sankce.

Další použitelná ustanovení trestního zákona v případě špionáže a sběru osobních dat:
§ 105 – Vyzvědačství, § 106, § 107 – Ohrožení utajované skutečnosti, § 125 – Zkreslování údajů o stavu hospodaření a jmění, § 149 – Nekalá soutěž, § 257a – Poškození a zneužití záznamu na nosiči informací (např. zkopírování seznamu zákazníků a jeho prodej konkurenční firmě).

Další právní normy zabývající se ochranou osobních údajů:

- ***Směrnice Evropského parlamentu a Rady o ochraně jednotlivců se zřetelem na zpracování osobních dat a o volném pohybu takových dat*** [48]. Snaží se mezinárodně vyrovnat s ochranou osobních údajů. Naplnění této směrnice bylo nutnou podmínkou pro vstup České republiky do Evropské unie.
- ***Směrnice Evropského parlamentu a Rady o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru.*** [50], která se týká zpracování osobních údajů a ochrany soukromí v telekomunikacích (tedy i Internetu).
- ***Štrasburská úmluva Rady Evropy na ochranu osob se zřetelem na automatizované zpracování osobních údajů*** [58].

6.3. Porušení soukromí elektronické pošty

Elektronické dopisy by měl uživatel zabezpečit, protože existuje reálné nebezpečí jejich přečtení či změny třetí osobou. Dalším problémem je pak pravost obdržené elektronické zprávy. Proti přečtení a změny třetí osobou se dá použít šifrování zpráv, pravost dopisu se dá zaručit elektronickým podpisem (kapitola 6.4.2.).

6.3.1. Ochrana důvěrnosti a formy elektronické pošty pomocí šifrování

Účinným způsobem, jak chránit soukromí dopisů posílaných prostřednictvím elektronické pošty, je použití šifrování, které aplikuje metody kryptografie. V informatice slouží kryptografie k ochraně soukromí dat, hlavně před jejich přečtením a modifikací. Také k ověření pravosti dokumentu.

Šifrování je proces, při němž se původní text pomocí kryptografického algoritmu a šifrovacího klíče přetransformuje do šifrovaného textu. Ten potom obecně vypadá jako náhodný shluk znaků. Dešifrování je proces opačný k šifrování. Šifrování lze využít při každodenním přenosu dat z jednoho počítače na druhý. V současné době se používají dva hlavní typy šifrovacích algoritmů:

1. Algoritmy s privátním klíčem: Pro šifrování i dešifrování se používá stejný klíč. Těmto algoritmům se také někdy říká šifry se symetrickým klíčem. Jako příklady systémů s privátním klíčem lze uvést AES, Blowfish, 3DES, Serpent.
2. Algoritmy s veřejným klíčem: Pro šifrování a dešifrování se používají dva různé klíče: veřejný a privátní klíč. Termín veřejný klíč vychází ze skutečnosti, že šifrovací klíč je možno klidně zveřejnit, aniž by se porušila bezpečnost zprávy nebo dešifrovacího klíče. Příklady šifrovacích algoritmů s asymetrickým šifrováním: RSA[20], DSA (Digital Signature Algorithm).

V prostředí Internetu se používá častěji šifrování s veřejným klíčem, jeho principy se uplatňují při bezpečné práci právě s elektronickou poštou a také se stávají součástí protokolů pro bezpečný přenos (např. SSL – Secure Sockets Layer).

Mezi používané šifrovací programy patří PGP, BestCrypt, FineCrypt, CryptoExpert, EasyCrypto Deluxe, Folder Crypt apod.

[20] Název odvozen ze jmen autorů: Rivest, Shamir, Adleman.

6.3.2. Legislativa

Zákon o poštovních službách [40]

Dle § 16 – Poštovní tajemství – má provozovatel nebo osoba podílející se na poskytování poštovních služeb povinnost zachovávat mlčenlivost o skutečnostech týkajících se poskytované nebo poskytnuté poštovní služby, které se při své činnosti dozvěděli.

Zákon o telekomunikacích [25]

Dle § 84 – Telekomunikační tajemství a ochrana osobních a zprostředkovacích dat – právnické nebo fyzické osoby, které vykonávají telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se podílejí na vykonávání telekomunikačních činností, nesmějí získávat pro jiné než pracovní účely, vyplývající z jejich telekomunikační činnosti, informace o skutečnostech, které jsou předmětem telekomunikačního tajemství ve větší míře, než je pro vykonávání telekomunikačních činností nezbytně nutné. Každý, kdo se dozví informace o skutečnostech, které jsou předmětem telekomunikačního tajemství, je povinen zachovávat o nich mlčenlivost.

Celkově platí, že ochrana pošty a jiné komunikace (včetně té elektronické) se vztahuje jen na dobu, v níž je zpráva přenášena. Ve chvíli, kdy je pošta doručena adresátovi, nevztahuje se na ni přísná ochrana s výjimkami výše uvedenými[21] a záleží jen na adresátovi, jak s doručenou zprávou naloží.

Trestní zákon [20]

Porušování tajemství dopravovaných zpráv řeší § 239 a § 240.

§ 239 (1) Kdo úmyslně poruší tajemství a) uzavřeného listu nebo jiné písemnosti, při poskytování poštovní služby nebo jiným dopravním zařízením, nebo b) zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením, bude potrestán odnětím svobody až na šest měsíců. (2) Pracovník provozovatele poštovních služeb nebo telekomunikační služby, který a) spáchá čin uvedený v odstavci 1, b) jinému úmyslně umožní spáchat takový čin, nebo c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou telefonicky, telegraficky nebo dopravovanou podobným způsobem, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

§ 240 (1) Kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch, a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu nebo telefonního

[21] Odposlech Policií ČR, Bezpečnostní informační službou apod.

hovoru, které nebyly určeny jemu, nebo b) takového tajemství využije, bude potrestán odnětím svobody až na jeden rok.
(2) Pracovník poštovní nebo telekomunikační služby (lze za něj považovat i poskytovatele připojení k Internetu), který a) spáchá čin uvedený v odstavci 1, nebo, b) jinému úmyslně umožní spáchat takový čin, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

Další právní norma chránící tajemství přenášené zprávy na Internetu:

- ***Zákon o ochraně utajovaných skutečností*** [39].

6.4. Falšování elektronických zpráv, WWW stránek a příspěvků v diskusních skupinách a konferencích

6.4.1. Ujištění se o pravosti elektronické zprávy

Obranou při podezření na zveličování či falšování informací v e-mailech je ověření jinou cestou (osobně či telefonicky).

6.4.2. Ochrana pravosti elektronické pošty elektronickým podpisem

Zatímco šifrování veřejným klíčem zabezpečuje dopis tak, že je jednak nečitelný, a také nezměnitelný, elektronický podpis zaručí pravost dopisu, aby se nedalo pochybovat o tom, že dopis odeslal skutečně ten, kdo se za něj vydává. Jedná se o problém autentizace.

Ze zprávy, kterou chce uživatel podepsat, se vygeneruje výtah zprávy (tzv. hash), který je kratší než samotná zpráva. Na druhou stranu však plnohodnotně charakterizuje její obsah. Mezi nejznámější algoritmy hashovacích funkcí patří MD2 a MD5. Hash se potom zašifruje veřejným klíčem (asymetrický algoritmus RSA) – provozovaným ovšem opačným směrem. Při šifrování veřejným klíčem se dešifruje privátním klíčem. Pokud se zpráva zašifruje privátním klíčem, její dešifrování je možné jen s pomocí párového veřejného klíče. Pokud je možno zprávu dešifrovat veřejným klíčem, pak to znamená, že byla zašifrována správným privátním klíčem, a to je vlastně základní princip digitálního podpisu.

Je-li použit na zprávu privátní klíč, plní funkci podpisu. Kombinací algoritmu privátního klíče a výtahu zprávy lze vypočítat digitální podpis odesílané zprávy. Když příjemce zašifrovanou hodnotu obdrží, může ji dešifrovat veřejným klíčem. Z obdržené zprávy si rovněž vytvoří výtah, a pokud se obě hodnoty shodují, pak má jistotu, že obdržel stejnou zprávu, která byla odesílána.

Princip používání elektronického podpisu:

- Získání programu pro vytváření a ověřování elektronického podpisu.
- Programem se vygeneruje dvojice soukromého a veřejného klíče.
- Předložení dokladů prokazujících totožnost a veřejného klíče poskytovateli certifikačních služeb. Vystavení veřejného klíče na WWW stránkách poskytovatele certifikačních služeb.
- Uživatel se již může podepisovat soukromým klíčem a příjemce podepsaného dokumentu si může ověřit jeho pravost.

6.4.3. Zjištění původce falšovaných materiálů

Jak zjistit pravou totožnost uživatele [2]:

- Údaje v hlavičkách e-mailových zpráv (e-mailové adresy).
- Obsah WWW stránek a jejich doménové jméno.
- Adresa serveru (IP adresa), na kterých se WWW stránky nacházejí.
- Telefonní čísla, z kterých se na server připojovalo.

Každý server, kterým e-mail projde, přidá do hlavičky zprávy řádek, ve kterém je napsáno, který počítač (název, IP adresa) mu zprávu poslal. Jedná se o řádky označené „Received:“. Některé adresy počítačů mohou být zfalšovány, ovšem ne ta poslední, protože server elektronické pošty zjistí, od koho zprávu dostal. IP adresa počítače, který zprávu poslal, určuje, z jakého stroje zpráva odešla nebo přes jaký šla. Lze tedy jít po hlavičkách „Received:“ a zjišťovat, zda jsou IP adresy pravé. Šikovný podvodník však umí změnit všechny řádky záhlaví, tudíž ani záhlaví vždy neobjasní pravý původ zprávy.

6.4.4. Phishing a pharming – znaky a obrana

Znaky:

- Špatná URL, např. www.bankovniustav.cz@52w3z259.yahoo.com.
- Obecná e-mailová adresa uživatele (banky obvykle píší svým klientům jmenovitě).
- Vyhrožování zrušením účtu.

Obrana:

- Nebýt příliš důvěřivý, být ostražitý a opatrný.
- Antivirový program a antispyware.
- DNS Blacklist (neboli seznam falšovaných IP adres).
- Ověřovat autenticitu druhé strany (certifikáty apod.).

- Personální firewall (viz kapitolu 6.9.).
- Správné nastavení a pravidelné aktualizace operačního systému a prohlížeče.
- Kontrola IP adresy příkazem WHOIS.

6.4.5. Legislativa k dokazování totožnosti původce činu

V případě, že byla nalezena osoba, která provedla nějakou nekalou činnost na Internetu, je důležité dokázat, že ona osoba byla opravdu tím pachatelem. Je možné, že počítač, ze kterého byl spáchán nějaký trestný čin, sdílí více osob. Dále je možné, že se pachatel vydává za jinou osobu.

Občanský soudní řád [22]
Dle § 125 v části věnovaným důkazním prostředkům mohou za důkaz sloužit všechny prostředky, jimiž lze zjistit stav věci, zejména výslech svědků, znalecký posudek, zprávy a vyjádření orgánů, fyzických a právnických osob, notářské nebo exekutorské zápisy a jiné listiny, ohledání a výslech účastníků.

Zákon o elektronickém podpisu [26]
Tento zákon charakterizuje zaručený elektronický podpis takto (§ 2 písm. b):

1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Pokud je elektronická zpráva opatřena elektronickým podpisem, je možnost útoku na takovou zprávu mnohonásobně menší. Rizikem je pak pouze porušení bezpečnostních pravidel poskytovatelem tohoto podpisu či samotným uživatelem.

Trestní řád [21][22]
Dle § 89 může za důkaz sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Podezřelého lze sledovat a odposlouchávat jeho komunikaci dle § 88 trestního řádu. Dále lze zajistit stopy v jeho počítači.

[22] Podobné interpretace v právních normách jako je správní řád [19], zákon o Bezpečnostní informační službě [37], zákon o státní kontrole [38] apod.

6.5. Porušování vlastnických práv

Vlastnictví jako pojem znamená možnost nakládat podle své vůle s tím, co je vlastněno. Specifikem duševního vlastnictví je, že předmět tohoto vlastnictví může používat více lidí a zároveň původnímu vlastníkovi nic fyzicky neubude. Proto se v případě duševního vlastnictví často nehovoří o krádeži, ale o kopírování. [1]

6.5.1. Ochrana duševního vlastnictví

Autorské právo (angl. copyright) je jednou z možností právní ochrany duševního vlastnictví. Jedná se o odvětví práva, které obsahuje nároky tvůrců autorských děl (spisovatele, hudebníky, filmaře, programátory apod.) na ochranu před nespravedlivým užíváním jejich tvorby. [13]

Do předmětů vlastnictví, na které se vztahuje autorská právní ochrana copyrightu, můžeme zařadit literární, vědecká, umělecká díla a software. Aby bylo na první pohled jasné, jaká díla jsou chráněna copyrightem, je vhodné je označit. Používá se symbol ©. Autorská práva se vztahují na každý soubor, který uživatel vytvoří (dokumenty, elektronická pošta, diskusní příspěvky, grafické soubory, zvukové soubory, webové stránky, software atd.). Předmětem autorského zákona jsou sice diskusní příspěvky, ale ne chat, protože nemá ustálenou formu (je podobný telefonování) a neukládá se do nějaké neměnné podoby [3].

Lidé si často neuvědomují, na co všechno se vztahují autorská práva, a porušují je. Lepší je, když se značka copyrightu © umístí na viditelné místo jako je nadpis, jméno autora apod. Není to nutné (díky Bernské dohodě viz kapitolu 6.5.2.), ale je to lepší. Dobré je si také značku zaregistrovat na úřadě pro ochranu autorských práv.

Ochrana softwaru copyrightem

Autor jako držitel copyrightu může definovat podmínky kopírování. Dle podmínek a omezení kladených na uživatele při používání softwaru, se software dělí do následujících skupin [1]:

- Copyboarding. Totální zákaz kopírování díla.
- Licensing. Dnes nejčastější způsob distribuce prodávaného softwaru, kdy se kupující zavazuje dodržovat určité licenční podmínky.
- Shareware. Je to téměř zdarma distribuovaný software, který není zbaven autorských práv a pravidel z toho vyplývajících. Při jeho používání je obvykle autorem vyžadován malý poplatek, za který uživatel dostane dokumentaci, doplňkové moduly apod.

- Copylefting. Vlastně jiné označení pro GNU General Public License (GPL), česky všeobecná veřejná licence GNU. Zdrojové kódy tohoto softwaru pod GPL mohou být volně používány a modifikovány, šířit se však mohou opět pod GPL.
- Freeware[23]. Označení zdarma šiřitelného programu. Program typu freeware dá veřejnosti k dispozici jeho autor s tím, že nevyžaduje žádné zvláštní poplatky za jeho použití. Je to jedna z metod, jak vlastní software prezentovat nekomerční a tedy i nenákladnou cestou.
- Public domain[24]. Označení pro software, který je určen pro veřejné použití. Takto označený program lze bezplatně používat, kopírovat a dále šířit. Na public domain software se nevztahuje ochrana pomocí copyrightu.
- Demoware. Volně šiřitelný software, který je limitovanou verzí komerčního programového systému. Cílem je, aby si uživatel mohl program vyzkoušet ještě před zakoupením. Repertoár funkcí je obvykle stejný jako u prodávané verze, ale fungování je nějakým způsobem omezeno (pouze do určitého data, stanovený počet dní ode dne instalace, počet spuštění apod.)

Ochrana WWW dokumentů copyrightem

Jedná se o ochranu vlastních WWW dokumentů, které může každý uživatel na Internetu publikovat. Ochranu WWW dokumentů můžeme rozdělit do více rovin. Jednak na ochranu obsahu WWW stránky, a pak také formy neboli použitého designu vytvořeného zdrojovým kódem pomocí jazyka HTML. Obsah je autorsky chráněn stejně jako díla typu časopis, kniha, atd. Forma WWW dokumentu je chráněna copyrightem v případě, že dokument je svým vzhledem a rozmístěním obsahových prvků originální a sofistikovaný oproti jiným dokumentům.

Ochrana příspěvků v diskusích a konferencích

Do copyrightu také spadají všechny příspěvky, které uživatel zašle do diskusních skupin a elektronických konferencí. Jedná se totiž o tvůrčí a originální dílo svého autora. Z toho vyplývá, že tutéž zprávu může do jiné diskusní skupiny zaslat pouze autor textu.

[23] Pojem freeware svádí k záměně za free software. Takto se ovšem označuje software, který může každý volně kopírovat, distribuovat i modifikovat. Software, který má splňovat toto označení, musí být k dispozici ve zdrojovém tvaru. Označení free software může původní autor kdykoliv změnit.

[24] Označení public domain se často mylně vztahuje na software typu freeware nebo shareware. Takto označované programy jsou ovšem chráněny copyrightem, jen jsou šířeny bezplatně.

6.5.2. Legislativa

Bernská úmluva o ochraně literárních a uměleckých děl [56]

Jedná se o mezinárodní smlouvu, která sjednotila přístup států k autorským právům. Byla několikrát upravována. Od roku 1967 tuto úmluvu spravuje Světová organizace duševního vlastnictví (WIPO[25]). Dle této dohody začíná zajištění autorskými právy automaticky okamžikem, kdy je dílo vytvořeno, i když se na něm nenachází copyrightová značka ©. Znamená to, že veškeré diskusní příspěvky, elektronická pošta, programy a webové stránky nejsou společným majetkem, pokud neobsahují sdělení, které je označuje za „společný majetek". Existují i další mezinárodní úmluvy na toto téma[26].

Směrnice Evropského parlamentu a Rady o harmonizaci některých aspektů autorských a souvisejících práv v informační společnosti [53]

Dle článku 3 navržená harmonizace pomůže naplnit čtyři svobody vnitřního trhu a uvádí do souladu základní zásady práva a zejména vlastnictví, včetně vlastnictví duševního, svobodu projevu a veřejný zájem.

Směrnice Rady o patentovatelnosti vynálezů realizovaných počítačem [46]

Tato směrnice stanoví pravidla patentovatelnosti vynálezů realizovaných počítačem. Dle článku 2, pro účely této směrnice se rozumí:

a) „vynálezem realizovaným počítačem" každý vynález, jehož provedení vyžaduje použití počítače, počítačové sítě nebo jiného programovatelného zařízení, přičemž tento vynález má jeden nebo více znaků, které jsou zcela nebo zčásti uskutečňovány prostřednictvím jednoho nebo několika počítačových programů;
b) „technickým přínosem" přínos ke stavu techniky v technické oblasti, který je nový a pro odborníka nevyplývá zřejmým způsobem ze stavu techniky. Technický přínos je hodnocen podle rozdílu mezi stavem techniky a rozsahem patentového nároku posuzovaného jako celek, který musí zahrnovat technické znaky, bez ohledu na to, zda jsou tyto znaky doprovázeny netechnickými znaky či nikoli.

Občanský zákoník [16]

Zajišťuje mimo jiné i ochranu duševního vlastnictví, protože upravuje majetkové vztahy fyzických a právnických osob, majetkové vztahy mezi těmito osobami a státem, jakož i vztahy vyplývající

[25] World Intellectual Property Organization.
[26] Např. Ženevská všeobecná úmluva o autorském právu [57].

z práva na ochranu osob atd. [2] Právní vztahy vznikající z výsledků duševní tvořivé činnosti upravují i další zvláštní zákony[27].

Autorský zákon [24]

Nový autorský zákon č. 121/2000 Sb. byl vytvořen hlavně s cílem sjednotit české autorské právo s mezinárodními principy a úmluvami[28]. V autorském zákoně se řeší otázka příslušnosti autorova díla k danému soudu. Na Internetu se rozlišuje právo státu původu díla a právo státu užití díla. Mělo by platit, že původ díla je v zemi, kde ho autor vystavil na Internetu. Země, na jejíž server autor dílo vystavil, je potom zemí užití díla.

§ 4 autorského zákona oznamuje, že prvním oprávněným veřejným přednesením, provedením, předvedením, vystavením, vydáním či jiným zpřístupněním veřejnosti je dílo zveřejněno. Zahájením oprávněného veřejného rozšiřování rozmnoženin je dílo vydáno. Prostřednictvím Internetu tedy dochází jak ke zveřejnění, tak k zpřístupnění díla veřejnosti na určité adrese Internetu.

Dle § 18 odst. 2 sdělováním díla veřejnosti je také zpřístupňování díla způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí.

Pravomoci získané dle tohoto zákona:

- Vytvářet libovolné množství kopií jakýmkoliv způsobem (§ 13).
- Distribuovat kopie – sám autor může kopie zdarma rozdávat, prodávat, pronajímat nebo zničit (§ 14 – 16).
- Vytvářet a distribuovat nové verze díla. Nové verzi se říká derivát.
- Dílo vystavovat, např. na WWW stránce (§ 17).
- Dílo sdělovat veřejnosti – živě či ze záznamu, rozhlasem, televizí apod. (§ 18 – 23).

K porušení autorských práv (angl. infringement) dochází ve chvíli, kdy jiný uživatel práci kopíruje šíří, upravuje nebo vystavuje. Taková činnost je nezákonná, i když není myšlena úmyslně nebo třeba ani nepřináší zisk.

[27] Zákon o vynálezech, průmyslových vzorech a zlepšovacích návrzích [31]; autorský zákon [24]; zákon o ochranných známkách [28]; zákon o užitných vzorech [32] apod.
[28] Bernská úmluva o ochraně literárních a uměleckých děl [56]; Ženevská všeobecná úmluva o autorském právu [57].

Některé body nového autorského zákona [2]:

- Oddělení osobnostních a majetkových práv.
- Nový autorský zákon platí, nedohodnou-li se smluvní strany jinak.
- Upravuje licenční smlouvu. Úprava je jednotná s obchodním zákoníkem.
- Upravuje nároky autora na neoprávněné užití jeho díla – povoluje stažení a zničení těchto kopií.
- Zákon se shoduje s některými souvisejícími právy Evropského společenství.
- Zaručuje větší ochranu autorům práv, kteří šíří svá díla moderními technologiemi.
- Zákon posiluje práva investorů, zaměstnavatelů a zavádí vedle zaměstnaneckých děl díla další[29].
- Zákon prodlužuje dobu ochrany autorských děl na 70 let po smrti autora a zaručuje jejich ochranu na celém území Evropské unie.

Co se týče počítačových programů, vymezuje je nový autorský zákon dle § 65 takto: Odst. 1: Počítačový program, bez ohledu na formu jeho vyjádření, včetně přípravných koncepčních materiálů, je chráněn jako dílo literární. Odst. 2: Myšlenky a principy, na nichž je založen jakýkoli prvek počítačového programu, včetně těch, které jsou podkladem jeho propojení s jiným programem, nejsou podle tohoto zákona chráněny.

Dle § 30 Volná užití platí: Odst. 1: Za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu. Odst. 2: Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla. Odst. 3: Užitím podle tohoto zákona je užití počítačového programu či elektronické databáze i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu.

V každém případě (až na volné freewarové programy) musí uživatel nabýt právo k užívání programu licenční smlouvou (§ 46). Licenční smlouvou dokazuje nabyvatel legalitu používání softwaru.

Díl 5 se zabývá ochranou práva autorského, kde dle § 40 se autor, do jehož práva bylo neoprávněně zasaženo nebo hrozí zásah, může domáhat:

- určení svého autorství,

[29] Úřední dílo, audiovizuální dílo, kolektivní dílo, školní dílo, soutěžní dílo, databáze.

- zákazu ohrožení svého práva,
- sdělení údajů o neoprávněně zhotovené rozmnoženině či napodobenině díla,
- odstranění následků zásahu do práva,
- poskytnutí zadostiučinění za způsobenou nemajetkovou újmu.

Nejčastěji diskutované problémy týkající se autorského práva se nacházejí v příloze č. 7.

Zákon o vynálezech, průmyslových vzorech a zlepšovacích návrzích [31]
Autorským právem chrání autor svůj výtvor před plagiátorstvím, patentem chrání autor svůj vynález před okopírováním. Patentové právo ochraňuje myšlenku, která je základem nějakého vynálezu. Užitný či průmyslový vzor chrání technické řešení a vzhled výrobku.

Zákon o přestupcích [23] – Přestupky proti občanskému soužití
Při poskytnutí vypáleného CD s materiály z Internetu někomu dalšímu, dopustí se uživatel přestupku dle § 32 odst. 1 písm. a) – Přestupky na úseku kultury, který praví, že přestupku se dopustí ten, kdo neoprávněně užije autorské dílo, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databázi. Za přestupek lze uložit pokutu do 15 000 Kč. Může být také porušen § 24 – Přestupky na úseku podnikání.

Trestní zákon [20]
Dle § 152 (Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi) trestního zákona se při porušování autorského práva, práv souvisejících s právem autorským a práv k databázi postupuje následovně. Odst. 1: Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty. Odst. 2: Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 značný prospěch, nebo dopustí-li se takového činu ve značném rozsahu (např. nákup programového vybavení do firmy pouze jedenkrát a použití jeho kopie na všechny počítače ve firmě). Toto ustanovení postihuje např. neoprávněné užívání počítačového programu, okopírování WWW stránek nebo jejich poškození nebo neoprávněný přístup k databázi.

K problematice poškozování autorských práv se váže také § 257a – Poškození a zneužití záznamu na nosiči informací.

6.6. Scamy a podvodníci slibující bohatství

Podvodům založených na pyramidových a Ponziho schématech by se měl člověk vyhýbat. Je důležité tyto podvodné praktiky rozpoznat a nezapojovat se do nich. V následujících kapitolách se nacházejí rady, jak tato podvodná schémata ihned identifikovat.

6.6.1. Návod jak poznat pyramidová schémata [3]

1. Fráze typu „Jak si rychle vydělat peníze“, „Práce z domu“ apod.
2. Tvar pyramidy: posílání peněz pár lidem, na oplátku pošlou peníze stovky lidí.
3. Pozor na druh zboží. Vyhnout se rozesílání peněz, obchodování s adresami, ať už pomocí e-mailu či CD-ROM.
4. Každý zákazník je obchodním zástupcem.
5. Pozor na tzv. „neomezené právo k šíření“. Jedná se o získávání zákazníků pomocí bezcenné zprávy.
6. Přítomnost tabulek znázorňující zisk.

6.6.2. Pozor na maskování pyramid za legální obchodování

Tento způsob podvodu se samozřejmě neprezentuje jako „pyramida“, ale vydává se za různé způsoby obchodování. Uživatel by si měl dát pozor na následující názvy, pod které se pyramidová schémata, např. v inzerátech, schovávají:

- Prodej seznamů adres (takové obchodování se seznamy adres nejsou legální).
- Rozdávání dárků (výměna peněžních darů mezi přáteli a známými).
- Inzerování faxem (rozesílání adres pomocí faxu nebo telefonicky).
- Skládání dopisů do obálek (se seznamy adres).
- Prodej elektronických seznamů adres.
- Prodej sharewaru.
- Tištěné zprávy.
- Loterie rozšířená po celém světě.
- Trička. Prodej kódů vytištěných na tričkách.
- Maskování za MLM (Multi-Level Marketing)[30]. MLM je zákonný.

[30] Způsob obchodování, který má pyramidovou strukturu. Účastníci MLM neboli distributoři pracují zároveň jako obchodní zástupci (prodej zboží zákazníkům) i jako rekruti (získávání zákazníků pro distribuci).

6.6.3. Znaky varující před podvodem [3]

1. Jako kontakt je uvedena anonymní e-mailová adresa. Je to sice legální, ale pokud někdo žádá po uživateli peníze, měl by udat pravou adresu.
2. Adresa s poštovní přihrádkou (P. O. BOX).
3. Neověřitelné citáty lidí, kteří něco vyhráli, získali velké peníze apod. Vymyšlená ocenění firem „služba roku“, „firma roku“ apod.
4. Velká písmena, vykřičníky, otazníky, znaky jako €, $, spousta nul v peněžních částkách atd.
5. Skrytá cena, služby „zdarma“, které po člověku žádají např. počáteční zálohu.
6. „Nabídka pro prvních 50 lidí.“ Podvodník vyprovokuje k rychlému jednání, aby mohl vybrat peníze a rychle zmizet.
7. Spousta informací o penězích a málo o práci.
8. Řečnické otázky: „Chcete být bohatý?“, „Chcete získat peníze?“, „Chcete být nezávislý?“, „Znáte značky CocaCola, BMW, SONY?“, „Víte, jak se stát milionářem?“ apod.

6.6.4. Obrana v případě krádeže

Uživatel, který se stane obětí krádeže, může postupovat v následujících krocích [3]:

1. Začít věc řešit ihned a přímo s konkrétním uživatelem. Může jít totiž jen o nedorozumění. Nespoléhat jen na e-maily. Vždycky existuje možnost, že zpráva nebude doručena. Lepší formou komunikace je telefon. Může se také stát, že praví podvodníci se schovávají za identitu někoho jiného. A oběť může křivě obvinit z podvodu nepravého člověka.
2. Určit škodu, kterou podvodný uživatel způsobil. Může dojít ke ztrátě peněz, zboží, dat, času, narušení soukromí nebo bezpečnosti, poškození pověsti, fyzické nebo psychické újmě. Je možné, že nezasáhne-li se proti podvodníkovi, vzniknou další škody. Ať už pro konkrétního uživatele či nové oběti podvodníka.
3. Rozhodnout se dle výše škody a podle vlastního úsudku, zda má smysl věc řešit. Pokud je škoda malá a nevyplatí se riskovat např. soudní výlohy a ztrácet čas, je tu možnost věc nechat být.
4. Shromáždit důkazy. Od elektronických zpráv s podvodníkem až po podací lístek z pošty. Všechny události si chronologicky zaznamenat.
5. Vyhledat informace a možnosti (Internet, instituce, porada s právníkem). Je možné se spojit se správcem pošty, systému nebo počítače podvodníka. Např. dle e-mailové adresy lze zjistit podnik nebo školu, kde dotyčný podvodník působí. Lze se obrátit na jeho nadřízené. Pomoci může i správce doménového serveru uživatelova počítače. Lze využít „whois“ klienta, který umožňuje vyhledávat informace o doménách (např. datum registrace, vlastníci), IP adresách

(jaké organizaci patří), autonomních systémech, hostech v Internetu aj. Z institucí může pomoci místní a státní policie, zastupitelé obce, Úřad pro ochranu hospodářské soutěže nebo třeba sdělovací prostředky. Došlo-li k podvodu prostřednictvím poštovního styku, požádat o pomoc organizaci, která poštovní transakci zprostředkovala (Česká pošta, DHL).

6. Není-li jiná možnost, opatřit si právníka a podat žalobu k soudu.

6.6.5. Legislativa

Trestní zákon [20]

Dle § 250c – Provozování nepoctivých her a sázek:

(1) Kdo provozuje peněžní nebo jinou podobnou hru nebo sázku, jejíž pravidla nezaručují rovné možnosti výhry všem účastníkům, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

Použitelný je také § 250 – Podvod: Kdo ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

Provozování těchto podvodů bývá doprovázeno naplněním § 125 – Zkreslování údajů o stavu hospodaření a jmění a § 148 – Zkrácení daně, poplatku a podobné povinné platby.

6.7. Podvody v nabízení zboží, služby

Podvody popsané v kapitole 5.2.3. uživatel musí co nejdříve rozpoznat a včas se jim vyhnout. Mezi jednoduché rady patří např. z jiných zdrojů si zjistit skutečnou cenu nabízeného výrobku či služby nebo využít zkušenějších uživatelů v diskusních skupinách a zeptat se na jejich názor. Legislativa je v tomto případě obdobná jako v kapitole 6.6.5.

6.8. Prodej běžně dostupných informací

Některé firmy nabízejí informace, jak získat úvěr. Úvěr však nenabízí, jen informaci o tom, jak ho získat. Stejné je to s aukcemi a dražbami. Podvodníci neprodávají přímo levné zboží, které se dá při těchto příležitostech získat, ale pouze informaci o tom, kde se dražby a aukce konají.

Pokud někdo prodává seznamy velkoobchodníků, jedná se zase o podvod, který láká kupující na nízké velkoobchodní ceny. Tytéž informace lze ale získat ve Zlatých stránkách či katalogových vyhledávačích na Internetu zdarma. Navíc ne všichni velkoobchodníci prodávají své zboží konečným spotřebitelům. Někdy je potřeba mít k obchodování s velkoobchodníky speciální licenci.

Na druhou stranu by měl uživatel tyto případy rozlišovat od situací, kdy je za běžně dostupné informace vhodné zaplatit. Jedná se o informace, které jsou běžně a zdarma zjistitelné, ale jejich vyhledávání a shromažďování by stálo spoustu času a energie. Jsou lidé, kteří do toho tu energii vložili, tudíž v této situaci od nich není neetické tyto informace prodávat a zpoplatňovat.

6.8.1. Informace zdarma na Internetu

V dnešní době lze zjistit na Intenretu téměř vše. Od různých návodů na výrobu, pěstování, recepty nebo třeba vládní informace (zákony, poplatky). A za nic není potřeba platit. To nejjednodušší, co může uživatel udělat, je použít webových vyhledávačů k nalezení informací, které potřebuje vědět. Příklady vyhledávačů: www.yahoo.com, www.google.com, www.seznam.cz, www.tiscali.cz atd.

Legislativa je obdobná jako v kapitole 6.6.5.

6.9. Škodlivý software

6.9.1. Programy chránící před škodlivým softwarem

Škodlivému softwaru se uživatel může bránit programy, jako jsou antiviry, firewall či antispyware (již popsáno v kapitole 6.2.3.).

Antivirové programy (antiviry) jsou programy vytvořené pro vyhledávání a ničení počítačových virů. Princip činnosti antivirů spočívá v jejich vyhledání, prevenci (včasnému zjištění) a odstranění škod (obnova napadených souborů a systému). Antivirový program je vždy o krok pozadu. Ve chvíli, kdy si uživatel instaluje poslední verzi svého antivirového programu, tak se do oběhu zaručeně dostaly další typy nových virů. Ne vždy jde zjištěný virus odstranit. Pak následuje reinstalace dat.

Mezi nejznámější a nejpoužívanější antivirové programy v současnosti patří např. AVG Anti-Virus, ClamAV, Norton AntiVirus, ESET NOD32 Antivirus, avast!, Zoner Antivirus,

Kaspersky Antivirus, BitDefender Antivirus, McAfee Antivirus, Dr.Web Antivirus (uživatelská rozhraní některých programů viz přílohu č. 5).

Firewall (příklad viz přílohu č. 6) je soubor opatření (realizovaný určitým HW a SW), která zabezpečují síť proti neoprávněnému přístupu zvenčí a proti úniku informací. Sleduje veškerou síťovou komunikaci, která není uživatelem povolena. V programu lze nastavit podrobná pravidla filtrování. Firewall umožňuje:

- řízení přístupu uživatele z vnější i vnitřní sítě,
- nastavení přístupových práv,
- odfiltrování nebezpečných služeb,
- soustředění bezpečnosti do jednoho komunikačního uzlu,
- zablokování nepřátelského mapování vnitřní sítě,
- audit legálních a nelegálních operací aj.,
- zajišťuje bezpečnost při vstupu nebo výstupu do/ze sítě, nezajišťují však bezpečnost dat během přenosu,
- plní funkci filtru, který rozhoduje o tom, co a kam bude přes něj propuštěno.

Firewall dělíme na síťový a osobní (personální).

Síťový firewall je umístěn na vstupu do počítačové sítě a odděluje počítače od Internetu. Na základě stanovených pravidel propouští pouze některé pakety síťové komunikace a jiné odmítá, nebo rovnou odstraňuje. Například síťový firewall může automaticky povolit přijetí určitých dat jen tehdy, pokud si je předtím některý z počítačů v síti vyžádal.

Personální firewall umožňuje uživatelům absolutní kontrolu výměny informací mezi jejich a dalšími počítači, jak v rámci lokální sítě, tak i na Internetu. Typickým příkladem hrozby je napadení škodlivým softwarem z vnitřku sítě z nezabezpečeného počítače nebo notebooku, z USB paměti apod. Personální firewall také snižuje riziko úniku osobních dat, blokuje pop-up okna, filtruje bannery, může zakázat cookies a spyware aj.

6.9.2. Automatická aktualizace Windows

Ochranu uživatele před škodlivým softwarem také posílí automatické aktualizace systému. Protože není možné vytvořit bezchybný operační systém, přicházejí na řadu různé balíky Service Pack,

které stávající již nainstalované systémy inovují, čímž odstraní dosud objevené chyby a přidají nové funkce.

Aktualizace a zdokonalení OS Windows pomocí tohoto balíčku jsou zaměřeny mimo jiné i na účinnější nastavení bezpečnosti, kdy je zaváděno silnější výchozí nastavení bezpečnosti a aktualizace s novými vlastnostmi a nástroji navrženými tak, aby uživatelé mohli lépe chránit své systémy a informace před hackery, viry a dalšími hrozbami. Jedná se o rozšíření ochrany sítě, zvyšování ochrany paměti, lepší zabezpečení e-mailové komunikace a umožnění bezpečnějšího prohlížení Internetu.

6.9.3. Legislativa

Trestní zákon [20]
Ve chvíli, infikuje-li pachatel něčí počítač či nosič počítačovým virem, dochází k naplnění skutkové podstaty § 257a[31] – Poškození a zneužití záznamu na nosiči informací. Dále samozřejmě můžou být poškozeny nehmotné informace, projevy osobní povahy, osobní údaje, obchodní tajemství, soukromí osob, autorská díla, utajované skutečnosti apod. Tyto nehmotné statky chrání paragraf tohoto zákona také.

6.10. Spamming

Boj proti spamu je aktuálním problémem a výzvou mnoha společností vyvíjejících software. Se spamem se dá bojovat centrálně pomocí různých prostředků v mail serveru, lokálně pomocí funkcí v e-mailovém klientu nebo pomocí různých programů, které rozšiřují funkčnost e-mailového klienta.

6.10.1. Antispam

U antispamu se tedy většinou používá řešení s předřazeným serverem, který se umísťuje před stávající poštovní server. Pokud je e-mail filtry procesního serveru posouzen jako spam, může být buď přímo zlikvidován, nebo přes originální poštovní server doručen adresátovi s tím, že je označen jako spam.

[31] Odst. 1: Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch a) takových informací neoprávněně užije, b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

Klasifikace e-mailů podle odesílatele

V rámci klasifikace e-mailů podle odesílatele se provádí zejména prověřování e-mailové adresy odesílatele, případně její pravosti apod. Zpravidla se používají tyto filtry:

- **Whitelisty** – kontrola podle lokálního seznamu e-mailových nebo IP adres považovaných za odesílatele legitimních zpráv. Pokud e-mail „spadne“ do tohoto seznamu, není již dále kontrolován žádnou z dalších metod.
- **Blacklisty** – kontrola podle lokálního seznamu e-mailových nebo IP adres považovaných za odesílatele nevyžádaných zpráv (spamu). Pokud e-mail „spadne“ do tohoto seznamu, je posouzen jako spam.
- **RBL** (Real Time Blocklist) a **DSBL** (Distributed Sender Blackhole List) dostupné z veřejných serverů – kontrola podle veřejných blacklist seznamů IP adres, které obsahují informace o serverech umožňujících nebo přímo šířících spam.
- **SPF** (Sender Policy Framework) je protokol, který se zaměřuje na to, aby administrátoři internetových domén mohli popsat své poštovní servery prostřednictvím záznamu SPF. Poštovní servery tak mohou odmítnout přijetí e-mailové zprávy, u které nemohou prokázat, že přicházejí ze schválených serverů.

Klasifikace e-mailů podle obsahu (textu)

V rámci klasifikace podle obsahu (textu) e-mailu se provádí vyhledávání určitých slov a frází typických pro spam přímo v textu zprávy:

- **Filtr regulárních výrazů** – vyhledává v textu e-mailu určitá slova a fráze typické pro spam pomocí tzv. regulárních výrazů. Jednotlivé nalezené výrazy jsou ohodnoceny určitým počtem bodů, který se postupně sčítá a statisticky vyhodnocuje. Pokud celkové bodové ohodnocení e-mailu překročí definovanou mez, je zpráva posouzena jako spam.
- **Bayesův filtr** – analyzuje text zprávy tak, že každému slovu je přiřazena určitá pravděpodobnost, která určuje, zda se jedná o spam, nebo o legitimní e-mail.

Další způsoby

- **Graylisting**. Předpokládá se, že pokud je e-mail odesílán relevantním poštovním serverem, bude v případě prvotního odmítnutí zprávy pokus o její doručení ve stanoveném čase opakován. Pokud je e-mail odesílán pomocí nástroje spammera, je pravděpodobné, že se o opětovné doručení již pokoušet nebude.

6.10.2. Další způsoby boje se spamem

- Uživatel může odpovědět na spam a sdělit inzerentovi, že si nepřeje být na jeho seznamu adres. Někteří inzerenti však používají k rozesílání spamu počítačové programy a je těžké jim zprávu doručit.
- Napsat správci sítě, kterou využívá inzerent, a stěžovat si.
- Zavést všeobecné podvědomí o tom, že spamming je špatná věc a spammer je zločinec.
- Přesvědčit poskytovatele Internetu, aby do smluv se zákazníky přidali zákaz spammingu pod pohrůžkou odpojení zákazníka od Internetu v případě porušení zákazu uvedeného ve smlouvě.

6.10.3. Legislativa

Zákon o regulaci reklamy a o změně a doplnění zákona o provozování rozhlasového a televizního vysílání [41]

Dle § 2 odstavce 1 písmene e) se zakazuje šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje; na šíření reklamy elektronickými prostředky a jeho omezení se vztahuje zvláštní právní předpis. Za reklamu, která obtěžuje, se považuje reklama směřující ke konkrétnímu adresátovi za podmínky, že adresát dal předem jasně a srozumitelně najevo, že si nepřeje, aby vůči němu byla nevyžádaná reklama šířena.

Zákon o některých službách informační společnosti [30]

§ 7 – Šíření obchodních sdělení:

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.

(2) Podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

(3) Nehledě na odstavec 2, pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů upravených zvláštním právním předpisem[32], může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích vlastních obdobných výrobků nebo služeb za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím

[32] Zákon o ochraně osobních údajů [27].

svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

(4) Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud

a) tato není zřetelně a jasně označena jako obchodní sdělení,
b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo
c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

Občanský zákoník [16]

§ 53 odst. 2 týkající se spotřebitelských smluv: Prostředky komunikace na dálku umožňující individuální jednání mohou být použity jen tehdy, jestliže spotřebitel jejich použití neodmítl. Pouze s předchozím výslovným souhlasem spotřebitele mohou být použity automatické telefonní systémy bez (lidské) obsluhy, faxové přístroje a automatické rozesílání elektronické pošty. Použitím těchto prostředků komunikace na dálku nesmí spotřebiteli vzniknout žádné náklady.

Tato část občanského zákoníku byla upravena podle směrnic Evropského parlamentu a Rady[33].

6.11. Nástrahy obchodování po Internetu

Celkově platí, že pro bezpečný obchod je nutné dodržet následující body [2]:

- Ověření totožnosti kupujícího a prodávajícího (identifikace a autentizace).
- Zajištění bezpečnosti při přenosu osobních a tajných dat.
- Zajištění provedení úhrady a bezpečnosti při jejím provedení.
- Zajištění bezpečnosti přenosu plnění (je-li v elektronické formě).

6.11.1. Konkrétní zásady bezpečného prodeje a nakupování [3]

- Neuskutečňovat transakci, pokud uživatel neuvede celé své jméno, přestože se obchod bude zdát velice výhodný.
- Svého obchodního partnera požádat o adresu a telefonní číslo. E-mailová adresa k vyhledání osoby v případě problémů nestačí. Telefonní číslo raději ověřit.

[33] Směrnice o elektronickém obchodu [52]; směrnice o ochraně spotřebitele v případě smluv uzavřených na dálku [49]; směrnice o soukromí a elektronických komunikacích [54].

- Neposílat peníze ani zboží na poštovní přihrádku místo adresy. V případě, že obchodní partner bude ke svému obchodování používat poštovní přihrádku, požádat ho o adresu a telefonní číslo.
- Zeptat se na vzhled a technický stav zboží. Při nákupu dražšího zboží si vyžádat fotografii.
- Neposílat velké sumy peněz předem, přestože placení předem vyjde celkově levněji než placení na dobírku.
- Při velké objednávce zprostředkovat transakci prostřednictvím třetí osoby nebo využít možnosti doručení na dobírku. Dobírka sice nezajišťuje stoprocentní jistotu (možnost doručení poškozeného zboží), ale je stále jistější než platba předem.
- Spolupracovat raději s lidmi, kteří pracují na renomovaných síťových počítačích známých firem či škol. V případě problémů se lze obrátit na jejich šéfy či učitele.
- Řádně zabalit posílané zboží.
- Nepřijmout viditelně poškozenou zásilku.
- Uchovat všechny dokumenty týkající se prodeje (inzerát, pošta, podací lístek, poštovní poukázky apod.)

6.11.2. Služby na dobírku

Tato služba funguje tak, že prodávající pošle balíček, za který kupující při jeho vyzvednutí zaplatí. Zprostředkovatel (Česká pošta, soukromé zasilatelské firmy) peníze od kupujícího doručí prodávajícímu. Poplatek platí odesilatel balíčku a zároveň příjemce peněz v jedné osobě. Dobírka řeší situaci, kdy se kupující nemůže vymluvit na to, že mu zásilka nebyla doručena. Dále je možné se vyvarovat tomu, že by prodávající přijal nekrytý šek.

Přesto má služba na dobírku nevýhody. Prodávající může v balíčku poslat nějaké bezcenné věci. Dalším problémem je, že kupující může zásilku odmítnout. V tomto případě prodávající hradí zbytečné náklady za poštovné.

6.11.3. Zprostředkování obchodu třetí osobou

Pokud dochází k obchodování finančně náročnějšího zboží, doporučuje se provádět transakci prostřednictvím třetí osoby. Kupující a prodávající pošlou peníze a zboží třetí osobě, která zboží odešle kupujícímu. Ten má několik dní na to, aby zjistil, že zboží odpovídá jeho představám. Poté dá pokyn třetí osobě, aby zaplatila prodávajícímu. Pokud zboží není v pořádku, zboží i peníze se vrátí původním odesilatelům. Tyto služby třetích osob jsou samozřejmě zpoplatněny a vybírají poplatek bez ohledu na to, dopadne-li transakce dobře nebo ne.

6.11.4. Černé listiny

Řešením podvodů by mohly být tzv. černé listiny, které by obsahovaly seznamy lidí, kteří se pokusili o podvodný obchod. Taková černá listina by byla čas od času zveřejňována nebo stále k dispozici k nahlédnutí. Velkým nedostatkem takových černých listin by však byla situace, kdy se na takový seznam dostane nevinný člověk a jeho pověst tím značně utrpí. Tvůrce takové listiny pak může být žalován. Takový tvůrce si nikdy nemůže být jist správností informací, které mu oběti podvodů poskytnou.

6.11.5. Legislativa

Legislativa týkající se elektronického obchodu se neliší (v hlavních rysech) od klasického obchodování. V posledních letech se při úpravách stávajících zákonů týkajících se obchodování na Internetu klade důraz na jejich kompatibilitu s normami Evropských společenství.

Směrnice Evropského parlamentu a Rady o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu [52]
Cílem této směrnice je zajištění integrace Evropských společenství v oblasti elektronického obchodu na vnitřním trhu a zajistit volný pohyb služeb mezi členskými státy. Jde hlavně o to, aby členské státy upravily své právní předpisy podle této směrnice, aby byla v souladu v rámci celého Společenství. Výsledkem by mělo být uzavírání smluv elektronickou cestou. I další směrnice Evropského společenství se týkají elektronického obchodu[34].

Občanský zákoník [16][35]
Hlava pátá: spotřebitelské smlouvy. Např. § 53 umožňuje smluvním stranám možnost uzavřít obchod bez fyzické přítomnosti smluvních stran, a to prostřednictvím tzv. prostředků umožňujících komunikaci na dálku. Odst. 7 však říká: Byla-li smlouva uzavřena při použití prostředků komunikace na dálku, má spotřebitel právo od smlouvy odstoupit bez uvedení důvodu a bez jakékoliv sankce do 14 dnů od převzetí plnění atd. Tento odstavec je však snadno zneužitelný. Spotřebitel může věc zakoupit, 14 dní pro svou potřebu používat (např. nějaké nářadí či módní doplňky), a pak ho může dodavateli vrátit.

[34] Směrnice Evropského parlamentu a Rady na ochranu spotřebitele v případě smluv uzavřených na dálku [49]; směrnice Evropského parlamentu a Rady o zásadách Společenství pro elektronické podpisy [51] atd.
[35] Novely občanského zákoníku vycházely mj. i z norem Evropských společenství, např. směrnice Rady o nekalých podmínkách ve spotřebitelských smlouvách [47]; směrnice Rady o ochraně spotřebitele při smlouvách sjednávaných mimo obchodní provozovnu [45]; směrnice Evropského parlamentu a Rady o ochraně spotřebitele z hlediska smluv sjednávaných na dálku [49].

Dle § 40 odst. 3 je právní úkon platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé. Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.

§ 614 odst. 3: Při zásilkovém prodeji přechází vlastnictví na kupujícího převzetím věci kupujícím na místě dodání jím určeném. Tímto je ošetřeno, když se zboží na své cestě ke kupujícímu ztratí.

Zákon o elektronickém podpisu [26]
Stanovuje podmínky akceptace elektronického podpisu jako důkazu autentizace (více viz kapitolu 6.4.5.).

Obchodní zákoník [17]
§ 278 říká, že na základě veřejného návrhu (např. formou prezentace na WWW stránce) je smlouva uzavřena s osobou, která v souladu s obsahem veřejného návrhu a ve lhůtě v něm stanovené, jinak ve lhůtě přiměřené, nejdříve navrhovateli oznámí, že návrh přijímá, a navrhovatel jí uzavření smlouvy potvrdí. Přijme-li veřejný návrh současně několik osob, může navrhovatel zvolit, kterému příjemci uzavření smlouvy potvrdí.

§ 596 - § 600 upravují vady na výrobku, povinnosti prodávajícího na ně předem upozornit a právo kupujícího dostat slevu, odstoupit od smlouvy, uhradit nákladů, které mu vznikly v souvislosti s vadami a s uplatněním odpovědnosti za ně atd.

Další důležité zákony upravující obchod na Internetu:

- ***Zákon o vynálezech, průmyslových vzorech a zlepšovacích návrzích*** [31].
- ***Zákon o užitných vzorech*** [32].
- ***Zákon o ochranných známkách*** [28].
- ***Zákon o ochraně spotřebitele*** [42] (§ 13 a § 19 upravují reklamace).
- ***Autorský zákon*** [24] (Upravuje autorství děl a převodu práv na tyto díla atd.; více v kapitole 6.5.2.).
- ***Zákon o ochraně osobních údajů*** [27] (Tento zákon upravuje ochranu osobních údajů fyzických osob a podmínky jejich ochrany a zpracování během obchodního procesu.).

Pokud je uživatel během obchodování podveden či okraden, má možnost se řídit pokyny v kapitole 6.6.4. Obrana v případě krádeže.

6.12. Cenzura a regulace obsahu WWW stránek

6.12.1. Legislativa

Listina základních práv a svobod [15]

Dle článku 17 odstavce 3 je cenzura nepřípustná. Na druhou stranu lze pachatele např. za šíření poplašných zpráv, propagování nesnášenlivosti, ohrožování mravnosti, propagace zločinu atd. v případě spáchání zločinu trestně stíhat, ale až po jeho provedení. Předběžná cenzura je však zakázána.

Zákon o regulaci reklamy a o změně a doplnění zákona o provozování rozhlasového a televizního vysílání [41]

Lze dle § 2 tohoto zákona zakázat reklamu, která by byla nepravdivá, byla v rozporu s dobrými mravy, urážela národnostní nebo náboženské cítění, propagovala násilí, snižovala lidskou důstojnost nebo využívala strachu. Zákaz platí pro reklamu a osoby do 15 let, pokud ohrožuje jejich zdraví nebo psychický a morální vývoj.

6.13. Neslušné chování na Internetu

6.13.1. Eliminace neslušného chování v diskusích

Nevhodné a neslušné chování některých diskutujících v diskusních skupinách a konferencích by se určitě změnilo, kdyby se museli přihlašovat do těchto skupin pod svým vlastním jménem. Spousta lidí ztrácí zábrany a chová se neeticky a neslušně jen z toho důvodu, že jim to anonymita dovolí. Mají pocit, že je nikdo nemůže vypátrat, a mají vlastně pravdu. Kdyby lidé v těchto diskusích a konferencích museli působit jen se svou pravou identitou a ne pod přezdívkami, nadávek a dalších neslušných projevů by jistě ubylo. Ale technicky je toto opatření nemožné.

Dalším řešením je správce těchto skupin, který je kompetentní neslušné příspěvky mazat a tím snížit exhibici lidí, kteří přišli do diskusní skupiny jen škodit, vylévat si zlost a čekat na to, jak budou ostatní reagovat. Na chatu existuje tzv. správce místnosti, který může nevhodně se chovajícího chatujícího buď vyhodit (tzv. kicking) nebo mu zakázat přístup (tzv. banning). V případě vyhození se může chatující zpět přihlásit do místnosti pod podmínkou, že už se bude chovat slušně. V případě zákazu se chatující již nemůže do místnosti přihlásit. Zákaz platí buď na omezenou dobu, nebo natrvalo. V ideálním případě by se uživatelé měli řídit pravidly v kapitole 4.2.

6.13.2. Jak rozpoznat trollování [3]

- Příliš mnoho zásadních chyb ve faktech, které mají donutit lidi je opravovat a vše uvést na pravou míru.
- Velmi kontroverzní témata prezentována fanatickým způsobem (např. na diskusním fóru určeném ženám vložit příspěvek, že každá vdaná žena by měla přijmout příjmení svého muže).
- Zpochybnění hlavního tématu diskusní skupiny nebo urážky čtenářů skupiny.
- Stále opakované staré spory, které tak nemohou utichnout.
- Crossposting neobvyklým a nepřátelským způsobem. Diskuse zabývající se názory protichůdnými než je téma diskusní skupiny.
- Anonymní adresa trolla.

6.13.3. Legislativa

Trestní zákon [20]

§ 174 Křivé obvinění

(1) Kdo jiného lživě obviní z trestného činu v úmyslu přivodit jeho trestní stíhání, bude potrestán odnětím svobody až na tři léta.

(2) Odnětím svobody na tři léta až osm let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 značnou škodu nebo jiný zvlášť závažný následek.

Dle § 206 – Pomluva – kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na 1 rok. Přísnější trest následuje, použije-li pachatel k rozšíření pomluvy nějaký účinný způsob (tisk, televize, rozhlas, také samozřejmě Internet).

§ 235 – Vydírání:

(1) Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody až na tři léta.

(2) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) spáchá-li takový čin nejméně se dvěma osobami,
c) spáchá-li takový čin se zbraní,
d) způsobí-li takovým činem těžkou újmu na zdraví nebo značnou škodu,

e) spáchá-li takový čin na svědkovi, znalci nebo tlumočníkovi v souvislosti s výkonem jejich povinnosti, nebo

f) spáchá-li takový čin na jiném pro jeho rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je bez vyznání.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt nebo škodu velkého rozsahu.

Zákon o přestupcích [23]

§ 49 – Přestupky proti občanskému soužití

(1) Přestupku se dopustí ten, kdo

a) jinému ublíží na cti tím, že ho urazí nebo vydá v posměch,

b) jinému z nedbalosti ublíží na zdraví,

c) úmyslně naruší občanské soužití vyhrožováním újmou na zdraví, drobným ublížením na zdraví, nepravdivým obviněním z přestupku, schválnostmi nebo jiným hrubým jednáním,

d) omezuje nebo znemožňuje příslušníku národnostní menšiny výkon práv příslušníků národnostních menšin,

e) působí jinému újmu pro jeho příslušnost k národnostní menšině nebo pro jeho etnický původ, pro jeho rasu, barvu pleti, pohlaví, sexuální orientaci, jazyk, víru nebo náboženství, pro jeho politické nebo jiné smýšlení, členství nebo činnost v politických stranách nebo politických hnutích, odborových organizacích nebo jiných sdruženích, pro jeho sociální původ, majetek, rod, zdravotní stav anebo pro jeho stav manželský nebo rodinný.

6.14. Nevhodný nebo nebezpečný obsah internetových stránek

Je několik možností, jak umístit webové stránky na Internet – a) umístění na vlastním serveru, b) placené umístění na cizím serveru, tzv. webhosting, c) neplacené umístění na cizím serveru po vyplnění dotazníku (umožňuje vyplnění nepravdivých dat). V prvních dvou případech lze pomocí IP adresy vypátrat vlastníka webového prostoru. Není tomu tak však v případě třetím. Navíc v prvních dvou případech se vlastník webového prostoru nemusí shodovat s autorem nebezpečných či nevhodných WWW stránek.

Hlavní věc je, že policii prý v boji proti nelegálnímu obsahu na WWW stránkách velice pomáhají oznámení obyčejných internetových uživatelů.

6.14.1. Cenzura

Ani na Internetu nelze porušovat svobodu člověka, svobodu jeho slova a právo na vyjádření. Proto řešením, které by omezilo existenci nevhodných a nebezpečných materiálů na internetových stránkách, nemůže být cenzura.

Jedinou možností, jak přistupovat k takto kontroverzním materiálům, je stejný přístup jako u ostatních médií. Ne tedy aktivní cenzura, která je v rozporu s ústavně garantovanou svobodou slova. Řešením je zásah proti tvůrci problémového obsahu v okamžiku, kdy ho zveřejní.

6.14.2. Ochrana dětí před nebezpečím Internetu

Dokud dítě nedovede rozlišit mezi „hodnými“ a „zlými“ lidmi, od kterých jim hrozí nebezpečí, mělo by s Internetem pracovat pouze pod dozorem rodičů. Z poznávání Internetu lze udělat rodinnou událost. Děti by měly být poučeny o nebezpečích, která jim hrozí na Internetu a rodiče by měli stanovit pravidla, za kterých budou děti Internet používat:

- Poučit dítě o tom, že uživatelé Internetu jsou opravdoví lidé, takoví, které může potkat i v reálném životě – a podle toho se k nim chovat.
- Ostatní uživatelé Internetu mohou být jiní, než se dělají. Na Internetu je snadné skrýt svou pravou totožnost.
- Nikdy neuvádět adresu a telefonní číslo.
- Nikdy nikomu neprozrazovat hesla.
- V případě, že se dítě dostane do nepříjemného rozhovoru nebo dostane podezřelý e-mail, mělo by to hned oznámit rodičům.
- Nedomlouvat si s internetovým kamarádem schůzku bez vědomí rodičů.
- Rodiče by měli mít představu o tom, co jejich dítě na Internetu dělá.
- Nainstalovat programy blokující přístup k nevhodným materiálům (Naomi 3.2.90 Family Safe Internet, Net Nanny, SurfWatech, Cyber Patrol).
    - Programy blokující přístup ke stránkám pouze pro dospělé.
    - Programy povolující přístup pouze na stránky „vlídné k dětem“.
- Zajímat se o to, jaké aktivity na Internetu dítě provozuje. Zjišťovat, s kým si dítě po Síti píše. Požádat dítě, aby rodičům ukázalo své oblíbené webové stránky a diskusní skupiny.

Nejlepší metodou, jak zabránit dětem v přístupu k nemravným a nebezpečným materiálům na Internetu, je jejich dobrá výchova. Nejdůležitější je promluvit si s dítětem na toto téma a nezapomenout, že lidé si prohlížejí takové materiály z vlastního rozhodnutí.

6.14.3. Legislativa

Směrnice Evropského parlamentu a Rady o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu [52]

Dle této směrnice není poskytovatel Internetu zodpovědný za obsah WWW stránek uživatele, pokud a) poskytovatel neví o tom, že se na těchto stránkách objevují závadné informace, b) nebo to zjistil a podniknul kroky k odstranění těchto informací. Zodpovědný je samozřejmě autor.

Zákon o regulaci reklamy a o změně a doplnění zákona o provozování rozhlasového a televizního vysílání [41]

§ 2 – Reklama zboží, služeb či jiných hodnot, jejichž šíření je zakázáno, je zakázána. Reklama nesmí obsahovat nepravdivé údaje[36], prvky, které by byly v rozporu s dobrými mravy, zejména prvky urážející národnostní nebo náboženské cítění, propagující násilí, prvky snižující lidskou důstojnost nebo využívající motiv strachu. Zakázané jsou také reklamy pro osoby do 15 let, pokud podporují chování ohrožující jejich zdraví a psychický nebo morální vývoj atd.

Trestní zákon [20]

§ 164 – Podněcování: Kdo veřejně podněcuje k trestnému činu nebo k hromadnému neplnění důležité povinnosti uložené podle zákona, bude potrestán odnětím svobody až na dvě léta.

§ 165 – Schvalování trestného činu: (1) Kdo veřejně schvaluje trestný čin nebo kdo veřejně vychvaluje pro trestný čin jeho pachatele, bude potrestán odnětím svobody až na jeden rok. (2) Stejně bude potrestán, kdo v úmyslu projevit s trestným činem souhlas

a) pachatele nebo osobu jemu blízkou odmění nebo odškodní za trest, nebo
b) na takovou odměnu nebo odškodnění sbírá.

§ 198 – Hanobení národa, etnické skupiny, rasy a přesvědčení

(1) Kdo veřejně hanobí a) některý národ, jeho jazyk, některou etnickou skupinu nebo rasu, nebo b) skupinu obyvatel republiky pro jejich politické přesvědčení, vyznání nebo proto, že jsou bez vyznání, bude potrestán odnětím svobody až na dvě léta.

§ 198a – Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

(1) Kdo veřejně podněcuje k nenávisti k některému národu, etnické skupině, rase, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků, bude potrestán odnětím svobody až na dvě léta.

[36] Viz také kapitola 6.15. – Prezentace nepravdivých a zavádějících informací na Internetu.

(2) Stejně bude potrestán, kdo se spolčí nebo srotí k spáchání činu uvedeného v odstavci 1.
(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo
b) účastní-li se aktivně činnosti skupin, organizací nebo sdružení, které hlásají diskriminaci, násilí nebo rasovou, etnickou nebo náboženskou nenávist.

§ 202 – Výtržnictví: (1) Kdo se dopustí veřejně nebo na místě veřejnosti přístupném hrubé neslušnosti nebo výtržnosti zejména tím, že napadne jiného, hanobí historickou nebo kulturní památku, hrob nebo jiné pietní místo anebo hrubým způsobem ruší přípravu nebo průběh organizovaného sportovního utkání, shromáždění nebo obřadu lidí, bude potrestán odnětím svobody až na dvě léta. (2) Odnětím svobody až na tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny.

V § 205 – Ohrožování mravnosti – se potom postihují osoby, které rozšiřují materiály neslušné, neuctivé, zvrhlé, podněcující násilí nebo nebezpečné chování apod. Běžná prezentace pornografie nelegální není, pokud provozovatel stránek s pornografií dokáže zamezit přístupu osob mladších 18 let.

§ 260: (1) Kdo podporuje nebo propaguje hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka nebo hlásá národnostní, rasovou, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob, bude potrestán odnětím svobody na jeden rok až pět let.
(2) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí nebo jiným podobně účinným způsobem,
b) spáchá-li takový čin jako člen organizované skupiny, nebo
c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu.

§ 261: Kdo veřejně projevuje sympatie k hnutí uvedenému v § 260, bude potrestán odnětím svobody na šest měsíců až tři léta.

§ 261a: Kdo veřejně popírá, zpochybňuje, schvaluje nebo se snaží ospravedlnit nacistické nebo komunistické genocidium nebo jiné zločiny nacistů nebo komunistů proti lidskosti, bude potrestán odnětím svobody na šest měsíců až tři léta.

6.15. Prezentace nepravdivých a zavádějících informací na Internetu

Není jednoduché zjistit, zda dané informace na webových stránkách jsou pravdivé, kvalitní a skutečně užitečné. Při posuzování se postupuje jako u ostatních médií.

6.15.1. Znaky při posuzování věrohodnosti informací na WWW stránkách [1]:

- Identifikace autora informace a možnost ho kontaktovat.
- Identifikace informace a jejího zdroje.
- Cílová skupina zdroje (laici či odborníci).
- Dřívější zkušenosti uživatele se zdrojem.
- Přesnost a vyváženost obsahu (široká oblast či úzce vymezený problém).
- Autorita autora. Informace na URL adrese nějaké známé firmy či organizace (včetně elektronických zástupců novin a časopisů) má větší váhu než názory nějakého uživatele na vlastních WWW stránkách (s adresou P. O. BOXU).
- Chyby (gramatické, typografické, faktické), zobecňování, přehánění, dvojsmysly.
- Úprava, struktura a design WWW stránek
- Zastaralé informace (včetně neplatnosti hypertextových odkazů), nepřítomnost data vytvoření či poslední aktualizace. Je nutná platnost a ověřitelnost informace.
- Názory a úvahy uživatelů versus fakta.
- Možnost v dokumentu vyhledávat.
- Střet zájmů a zkreslené informace organizací o svém působení.
- Klamání, výhodné nabídky – na místě je obezřetnost uživatele.
- Recenzování a hodnotící služby obsahu WWW stránek (např. na www.excite.com, www.ipl.org, www.pointcom.com).
- Kvalita a platnost odkazů, přehledná navigace. Rozlišovat původní zdroje od pouhých odkazů na jiné zdroje.
- Uživatelská přívětivost, srozumitelnost a snadnost používání, rozsah informace.
- (Ne)snadnost připojení, (ne)dostupnost.
- Placený zdroj.
- Je nutné při posuzování kvality zdroje používat vlastní úsudek a nabyté znalosti.
- Zveřejňování nedodělaných dokumentů s nápisy „under construction“.

6.15.2. Boj proti Google bombě

- Zakázat indexování stránky, která se objevuje na hanlivé heslo „XY“ v souboru robots.txt. Robots.txt je textový soubor, který umožňuje autorovi webových stránek zakázat přístup některých botů (např. Googlebot). Nevýhodou ale je, že lidé při použití daného vyhledávače a korektní fráze nenaleznou oficiální stránky a budou zrušeny i zpětné odkazy. Další nevýhodou je, že na jiné vyhledávače zákaz neplatí.
- Další možností je zaplatit si reklamu v Google AdWords. Tato reklama by vysvětlila, jak to s hanlivým heslem „XY“ opravdu je a že se opravdu nevztahuje k dané osobě, instituci či skupině osob na vyhledaných webových stránkách.
- Další a nejúčinnější strategickou ochranou je budování značky, oblíbenosti a dobré pověsti, kdy pozitivní odkazy budou vždy převažovat nad těmi negativními.

6.15.3. Legislativa

Trestní zákon [20]

§ 199 – Šíření poplašné zprávy

(1) Kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá, bude potrestán odnětím svobody až na jeden rok nebo peněžitým trestem.

(2) Kdo zprávu uvedenou v odstavci 1, ač ví, že je nepravdivá a může vyvolat opatření vedoucí k nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa, sdělí podniku nebo organizaci nebo policejnímu nebo jinému státnímu orgánu anebo hromadnému informačnímu prostředku, bude potrestán odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2 opětovně, nebo způsobí-li takovým činem vážnou poruchu v hospodářském provozu nebo hospodářské činnosti podniku nebo organizace nebo v činnosti státního orgánu anebo jiný zvlášť závažný následek.

§ 200 – Kdo za stavu ohrožení státu nebo za válečného stavu způsobí, byť i z nedbalosti, nebezpečí vážného znepokojení, malomyslnosti nebo poraženecké nálady alespoň u části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, bude potrestán odnětím svobody na šest měsíců až tři léta.

Následující ustanovení neošetřují jen prezentování prostřednictvím vyvěšení informací na WWW stránkách, ale řeší také problematiku spammingu a hoaxových zpráv v kapitole 6.10.

6.16. Jak odhalit skutečnou identitu

Existují různé postupy, kdy se dá z textu odhalit skutečná identita člověka, který na Internetu předstírá jinou identitu. Například když tvrdí, že mu ještě nebylo patnáct let, a přitom používá knižní tvary. Na druhou stranu se může jednat o záměr, jak zmást ostatní uživatele. Pokud taková „falešná osoba“ zjistí, že po něm někdo pátrá, snadno může navést na falešnou stopu dalším předstíráním.

Nejčastější chyba, kterou lidé dělají je, že se opakují. Nemají připravený scénář s reakcemi. Věty totiž z nich nevycházejí intuitivně, tudíž potřebují čas pro své reakce. Kdo tuto hru neovládá dobře, opakovaně pak reaguje stejně s těmi samými slovy. Obecně platí, že když se někdo vydává za někoho jiného (např. muž za ženu), své reakce přehrává. Protože potlačit to, co je člověku přirozené, je těžké.

Zjišťováním skutečné totožnosti na základě textu psaného člověkem se zabývá forenzní (soudní) psychologie. Využívá se i v kriminalistice, kde pomáhá zjistit autora anonymního dopisu. Policejní metody se dají použít i na uživatele Internetu. Lze s danou pravděpodobností identifikovat pohlaví autora textu dle slov a stavby vět. Žena například píše jemněji. Je to znát ze slohu. Používá také více zdrobnělin. Ženy si dávají záležet na správné formulaci a text po sobě kontrolují spíše než muži. Ženy také používají více výplňových slov a do textu vkládají více citu. Muž píše rovnou k věci. K takovému rozboru, jaký používají kriminalisté, je však potřeba delší souvislý text. [12]

Pravou totožnost autora lze také zjistit zkoumáním, kde všude se vyskytuje přezdívka autora a zda ji používá ta samá osoba. Každý má specifický druh vyjadřování a úpravy textu (používané smajlíky – viz přílohu č. 2, druh a velikost písmen apod.). Lze si všimnout, zda nezmínil svou školu, zaměstnání, rodinu, město a zda si ve svých výrocích neodporuje. Dá se zjistit, kdy usedá k počítači či v jakých situacích znervózní, zda reaguje okamžitě nebo při chatování pracuje, zda dělá překlepy či dokonce opakované překlepy.

Většina lidí se na Internetu chová slušně, tudíž není důvod všem ostatním uživatelům předem nedůvěřovat. Přesto je důležité si dávat pozor na následující podezřelé znaky:

- Je podezřelé, zná-li internetový „známý“ o uživateli více, než o sobě sám zveřejnil.
- Velmi osobní nebo neslušné návrhy.

Dobré je se s dotyčným spojit telefonicky, vyměnit si fotografie (a doufat, že budou pravé) a v případě setkání se sejít na veřejném místě.

6.17. Neoprávněná registrace doménového jména

Účinnou radou proti „vykradení“ doménového jména jinou osobou je registrace jména jako ochranné známky. Doménová jména by měla být registrována jako ochranná známka a v České republice by se o to měl starat Úřad průmyslového vlastnictví. Jinak doménová jména lze považovat za duševní vlastnictví, která majitel domény vymyslel, a tudíž se na něj vztahuje ***autorský zákon*** [24].

6.17.1. Legislativa

Občanský zákoník [16]

Mimo jiné i občanský zákoník může pomoci řešit otázku přidělování doménových jmen (§ 11 Jméno a příjmení osoby, § 19b Název právnické osoby)[37]. Při přidělování doménového jména se s osobou, ať už fyzickou či právnickou, sepíše Smlouva o registraci doménového jména, která dle občanského zákoníku může být brána jako a) příkaz k provedení určité činnosti (§ 724), nebo b) by mohlo jít o smlouvu o dílo ve smyslu dosažení určitého výsledku (§ 631). Každopádně práva zúčastněných jsou nejasná a platí, že přidělování domén lze pojímat dvěma způsoby [2]:

1. Právní vztah mezi správcem a žadatelem založený na smlouvě mezi dvěma stranami.
2. Technologický postup, kdy se číselnému označení adresy přiděluje jméno domény.

Co se týče registrace domény s jiným jménem (např. veřejně známé osoby), na tuto situaci se vztahuje ochrana dle § 11 a § 13 (u právnických osob § 19b). Říkají, že fyzická osoba má právo mimo jiné i na ochranu svého jména a může se domáhat, aby bylo upuštěno od neoprávněných zásahů do práva na ochranu její osobnosti atd. Tato osoba je pak oprávněným registrátorem domény, jejíž název bude stejný se jménem fyzické osoby. Případně se může jednat o jinou osobu, ale tato osoba může registraci provést pouze se souhlasem osoby, jejíž jméno doména nese. Pokud uživatel zaregistruje doménu se jménem někoho jiného, je oprávněn ji používat do okamžiku, kdy se ozve první osoba, jejíž jméno se jménem domény souhlasí.

Při neoprávněné registraci jména právnické osoby jako domény se lze domáhat u soudu pozdržení jejího používání cizí osobou, odstranit tento stav a požadovat odpovídající kompenzaci (§ 53 obchodního zákoníku [17]).

[37] Jména a příjmení fyzických osob a názvy právnických osob dále upravují: zákon o matrikách [43]; zákon o užívání a změně jména a příjmení [44]; obchodní zákoník [17]; zákon o živnostenském podnikání [18] atd.

V České republice se dají na přidělování doménových jmen naštěstí aplikovat zákony, které chrání jména obchodních firem a ochranné známky[38]. Přihlásí-li někdo jméno domény, kterou ani neplánuje v nejbližší době registrovat, jako ochrannou známku, může se to brát jako jakási forma rezervace. Ale není zárukou, že by taková forma „rezervace" opravdu fungovala, navíc musí být splněno několik požadavků ze zákona o ochranných známkách.

Zákon o ochranných známkách [28]
Dle § 1 je ochrannou známkou označení tvořené slovy, písmeny, číslicemi, kresbou nebo tvarem výrobku nebo jeho obalu, popřípadě jejich kombinací, určené k rozlišení výrobků nebo služeb pocházejících od různých podnikatelů a zapsané do rejstříku ochranných známek, vedeného Úřadem průmyslového vlastnictví. Ochranná známka je chráněna ve spojení s konkrétními výrobky a službami, které je odlišuje od výrobků a služeb téhož druhu. Majitelem ochranné známky může být jen podnikatel.

Doménová jména, která jsou shodná či podobná s obchodním jménem, registrovanou ochrannou známkou nebo dlouhodobým označením někoho jiného, porušují práva a jsou přinejmenším v rozporu s dobrými mravy soutěže (jedná se o nekalou soutěž dle § 44 obchodního zákoníku). Na druhou stranu není povoleno, aby registrátor doménových jmen názvy jakkoliv cenzuroval.

Trestní zákon [20]
V případě, že jedna firma tajně skryje názvy výrobků chráněných jako slovní ochranné značky na stránkách konkurence tak, že při hledání těchto výrobků na Internetu jsou nalezeny stránky s nabídkou konkurenčních výrobků, jedná se o nekalou soutěž, která porušuje jak obchodní, tak i trestní zákoník (§ 151 Porušování průmyslových práv).

V případě, že někdo užije pro jméno své domény na Internetu název chráněný ochrannou známkou, kterou zaregistroval někdo jiný, porušuje tím § 150 – Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu.

V případě, že je někomu za úplatu nabízeno doménové jméno od někoho, kdo na toto jméno nemá nárok, může se jednat dokonce o trestní čin vydírání – § 235.

[38] Zákon o ochranných známkách [28].

7. Shrnutí reálných hrozeb a ekonomické zhodnocení

Internet není ve skutečnosti tak nebezpečné místo, pokud uživatel provede pár jednoduchých bezpečnostních opatření. Existují nepříjemnosti, u kterých je pravděpodobné, že se mu při práci s Internetem přihodí. Na druhou stranu existují hrozby, se kterými se uživatel při normálním chování na Internetu nikdy nemusí setkat. Jedná se o hrozby, které sdělovací prostředky v honbě za senzací zbytečně nafukují a přehánějí a zbytečně tím uživatele Internetu zastrašují. Takové zastrašování může vést u někoho až k tomu, že strach z crackerů a podvodníků nedovolí uživateli naplno využít výhod internetové sítě.

Tato kapitola by tedy měla vyhodnotit, s jakými reálnými hrozbami se běžný uživatel může potkat a na které by se tedy měl zaměřit. Jedná se o takové situace, které ho opravdu mohou ohrozit, protože pravděpodobnost setkání s nimi je vyšší. Zároveň tato kapitola využívá získaných poznatků z výše uvedených kapitol 5 a 6.

7.1. Hrozby – pravděpodobnost útoku a společenská nebezpečnost

Vždy, když se uživatel připojí k Internetu, riskuje tím, že přijde o část svého soukromí. Vždy tu bude možnost, že se nějaký cracker bude chtít dostat přes internetovou síť k jeho počítači, ať už pro zábavu, aby si dokázal, kam až může zajít, nebo proto, aby uživateli uškodil nebo získal nějaká data. Útoky crackerů, kde jde o peníze, jsou nejnebezpečnější. Stále bude existovat možnost, že někdo bude chtít pomocí spywaru získat o uživateli osobní informace.

Pořád je možné, že si někdo přečetl nebo změnil jeho odeslanou či přijatou elektronickou zprávu, pokud není zašifrovaná, nebo se za něj někdo bude v internetových vodách vydávat. Nelze si myslet, že se ho takové hrozby netýkají a doufat, že jemu se vyhnou. Soukromá data uživatelů začínají být vzácným zbožím a leckdo se nezastaví před nejrůznějšími špinavými taktikami, aby je získal. Za obzvláště nebezpečné považuji phishing a pharming. Hlavně u pharmingu má uživatel malou šanci na jeho odhalení a škody mohou být obrovské.

Internet je skvělým prostředím pro porušování autorských práv, a taky je toho ve značné míře zneužíváno. Krádeže a kopírování duševního vlastnictví probíhají na Internetu ve velkém. Společenská nebezpečnost se liší případ od případu. Rozdíl je mezi firmou, kde zakoupili jednu

licenci programu a používají ho na 20 počítači, a mezi člověkem, který používá nelegálně získaný textový editor k psaní domácích úkolů.

Vždycky existovali lidé, kteří se budou snažit vydělat na naivitě jiných. Internet se sice nehemží podvodníky, jak tvrdí média, ovšem tak jako v reálném životě existují i na Internetu, jehož výhody jim podvodné taktiky jenom ulehčují. Ale používá-li uživatel zdravý rozum a nevěří podvodníkům jejich výroky o „senzačně rychlém zbohatnutí“ nebo „zázračném vyléčení“, neměl by se nechat podvodníkem nachytat, protože místo rychlého zbohatnutí by mohl rychle o peníze přijít.

K nejčastějším a nejrozšířenějším neetickým problémům na Internetu patří produkce a rozšiřování škodlivého softwaru (počítačové viry, spyware, trojské koně, počítačoví červi, adware, dialer, keylogger). Proti tomuto softwaru se však dá bránit (viz další kapitolu 7.2.). Je pravda, že sdělovací prostředky a firmy prodávající antiviry, firewally apod. situaci schválně zveličují, ale není radno škodlivý software tohoto typu podceňovat, protože jeho působením může dojít k vysokým škodám a nákladům k jejich odstranění (viz kapitolu 5.2.5.).

Dalším velice častým nešvarem Internetu patří spamování a rozesílání nevyžádaných reklam. Přestože se jedná o nezákonnou činnost, nedaří se ji ani omezit, natož úplně zastavit. Opak je pravdou, protože spamování se stále rozšiřuje. Míra nebezpečnosti spamování není vysoká, ale přesto je uživatel okrádán o čas a kapacitu poštovní schránky. Spammer může schránku zahltit a způsobit nedoručení důležitého e-mailu. Nebo v budoucnosti dokonce zkolabování elektronické komunikace (viz kapitola o budoucnosti spamování 8.7. Spamming).

Kdo obchoduje přes Internet, může se samozřejmě setkat s tím, že jeho obchodní partner bude podvodník. Ale stejně se děje i v jiných formách obchodování. Podvodníci se najdou všude, ať už s nimi člověk obchoduje internetovou či jinou cestou. Z vlastní zkušenosti, ze zkušenosti mých známých a diskutérů, se kterými jsem toto téma probírala v internetových diskusích a také z poznatků různých autorů (jejich zkušeností popsaných v literatuře) musím konstatovat, že drtivá většina všech obchodů přes Internet probíhá bez problémů. Přesto by měl člověk důvěřovat, ale prověřovat, což u neznámých lidí platí dvojnásob.

Občas se stává, že se uživatel Internetu stane svědkem, někdy dokonce účastníkem různých hádek, válek, vášnivých výměn názorů a vulgárních projevů. Toto téma jsem opět diskutovala v internetových diskusích a i z vlastních zkušeností musím říct, že se bohužel nejedná o nic

neobvyklého. Pokud uživatel není např. veřejně pomluven nebo křivě obviněn, nejedná se o nic závažného, ovšem přesto tím přichází o drahocenný čas.

Problém nebezpečného obsahu WWW stránek je tu bohužel od počátku komerčního využívání Internetu. Např. různá hnutí, sdružení a sekty využívají možností Internetu k prezentaci své často nezákonné činnosti a výroků. Velkým problémem je dětská pornografie a podněcování k násilí. Tato trestná činnost se řadí k těm nejvíce nebezpečným a dle trestního zákona [20] se za ni také dávají vysoké tresty. Pokud ale uživatel takové materiály nevyhledává a bude dosaženo toho, že ani děti se k takovým materiálům nedostanou, přímo ho to neohrožuje. V případě nalezení webových stránek problematického charakteru je nutné skutečnost ohlásit Policii ČR, a tím proti tomuto materiálu bojovat.

Co se týče prezentování nějakých nepravdivých informací ať už na WWW stránkách nebo prostřednictvím chatu či elektronické pošty, přímo uživatele neohrožuje, pokud mu však nepřímo nezpůsobí nějakou škodu. Různých fám, spekulací, žertíků či výmyslů je však v internetové síti plno. Totéž platí o změně identity, kterou využívají hlavně diskutéři a chataři v chatech a diskusích. Změna identity není nebezpečná, někteří psychologové tvrdí, že je dokonce prospěšné občas se vtělit do nějaké jiné sociální role. Samozřejmě se nejedná o případ změny identity obchodníka-podvodníka, který se vydává za někoho jiného, aby okrádal.

Pokud si někdo neoprávněně registruje doménové jméno (např. fyzická osoba požádá o registraci doménového jména www.plzensky-kraj.cz), je to přinejmenším neetické. V případě, že by tato osoba požadovala za přenechání doménového jména od Plzeňského kraje úhradu, může jít dokonce o trestný čin vydírání. V případě právnických osob může jít o nekalou soutěž dle § 44 obchodního zákoníku [17].

7.2. Opatření a náklady

Opatření uvedená v této kapitole pomáhají běžnému uživateli snížit rizika spojená s používáním Internetu na minimum. Kombinací několika programů (které lze pro domácí použití získat zdarma) s několika bezpečnostními zásadami si uživatel může být téměř jistý, že ho nic nepřekvapí. Navíc pokud se uživatel bude průběžně zajímat o aktuální problematiku Internetu, získá cenné zkušenosti a bude věnovat pozornost elementům, které ho prostřednictvím Internetu ohrožují.

Aktualizace

Je dobré pravidelně aktualizovat operační systém počítače. Aktualizace obsahují různé záplaty, vylepšení a bezpečnostní opravy systému, jehož děr a nedokonalostí by mohl potenciální útočník využít. Za aktualizace uživatel neplatí. Aktualizace pro operační systém Windows se nachází na těchto webových stránkách:

http://update.microsoft.com

Dále se vyplatí aktualizovat svůj webový prohlížeč, poštovní a další programy.

Antivirový program

Nejúčinnější obranou proti virům je instalace a pravidelná aktualizace antivirového programu. Mnoho antivirů je pro domácí užití zdarma, např.:

AVG Anti-Virus Free edition	http://free.grisoft.com/
avast! 4 Home Edition	http://www.avast.com/
ClamWin	http://www.clamwin.com/

Ochrana proti spyware a adware

Bojovat proti spyware (a popř. adware) lze např. pomocí programů:

Spybot – Search & Destroy	http://www.slunecnice.cz/sw/spybot/
Ad-Aware SE Personal Edition	http://www.lavasoftusa.com/software/adaware/
AVG Anti-Spyware Free	http://free.grisoft.com/doc/download-free-anti-spyware/

Použití uvedených programů je pro domácí užití bezplatné.

Ochrana proti útoku

Proti neoprávněnému přístupu „zvenčí“ a úniku informací ochrání uživatele firewall. Firewall lze zapnout na ADSL modemu nebo routeru, pokud ho obsahuje. Naproti tomu lze použít i softwarový firewall. Pro domácí použití ho lze pořídit i zdarma (např. http://www.sunbelt-software.com/). Základní firewall obsahuje i operační systém Windows (příloha č. 6).

ZoneAlarm Free Firewall	http://www.zonealarm.com/store/content/catalog/products/sku_list_za.jsp

Používat zdravý rozum

- Neotvírat soubory a programy z pochybných zdrojů (pozor na přílohy elektronické pošty s příponami .exe, .bat, .vbs, .com).
- Vypnout služby http, FTP a telnet v případě, že nejsou používány.
- Používat důmyslná hesla všude, kde je to možné.
- Šifrování souborů v počítači i elektronických zpráv.
- Pod žádnými záminkami nesdělovat ostatním své osobní údaje, hesla apod.
- Pozor na phishing a pharming!
- Nenechat se vyprovokovat a vtáhnout do internetových hádek.
- Nevěřit všemu, co se píše na Internetu.
- Kvalitní antispam (filtry třídící elektronickou poštu dle odesilatele, obsahu apod.).

8. Budoucnost a trendy

S rozšiřováním technologií roste i počet prostředků pro páchání trestné činnosti, nové právní delikty, nové důkazy, nové triky zločinců. Je například velice těžké vypátrat a dopadnout někoho, kdo spáchal čin v jednom státě na serveru jiného státu, poškodil uživatele dalších národností a zároveň se ukrývá v úplně jiném státě. Spolupráce zemí v tomto případě vždy není zaručena. Řešením by měly být mezinárodní dohody. Lidé se neumí okamžitě bránit nějakému novému druhu deliktu, protože ani oni, ani legislativa na něj ještě nejsou připraveni. Proto je důležité se zaměřit na prevenci a ochranu.

8.1. Zneužívání anonymity

Lidé jsou stále více závislí na informačních technologiích, zahrnujících i internetovou síť, tudíž rostou i požadavky na bezpečnost v této oblasti a ochranu před zločinci. Anonymita a vzdálený přístup k počítačům, který Internet umožňuje, je dobrým předpokladem pro utajení člověka, který nemá v jednání s ostatními čisté úmysly. Situaci v páchání škodlivé a trestné činnosti na Internetu by mohla zlepšit nová kvalitnější a konkrétnější legislativa, nebo alespoň úprava té stávající, aby se již existující zákony daly bez problémů aplikovat na internetovou trestnou činnost. Částečným řešením by také mohly být zvýšené trestní sazby za internetové trestné činy, aby si uživatelé konečně uvědomili, že si v tomto prostředí nemohou dělat, co chtějí a že jejich svoboda jednání končí tam, kde začínají zákony.

Na jednu stranu je anonymita Internetu užitečná, protože lidé se mohou volně pohybovat, bavit se a svobodně vyjadřovat své názory. Na druhou stranu se jedná o dokonalé prostředí pro neetické a ilegální činnosti, které vzniknou a zmizí, aniž by byl zjištěn pachatel.

V poslední době je zřejmý trend upřednostňování specializovaných a soukromých diskusních skupin před těmi velkými a anonymními. Z tohoto příkladu je vidět, že lidé více přebírají odpovědnost nad svým chováním na Internetu a využívají ho s cílem se více vzdělávat, vyměňovat své názory apod.

Nedorozumění a používání falešné identity bude v budoucnosti omezeno setkáními se zvukem a obrazem (prostřednictvím webové kamery). Tzv. smajlíky (smilies – viz přílohu č. 2) vymizejí, protože emoce budou uživatelé vyjadřovat přímo verbálními i neverbálními prostředky. Ale je

možné, že nakonec vzniknou technologie, které i při takových živých setkáních umožní skrývat pravou identitu.

8.2. Bezpečnostní trendy

Kapitoly 6.1.1. a 6.1.2. se zabývaly bezpečnostními pravidly Bezpečí při velkém počtu a Bezpečí díky neznalosti. Na ně se v budoucnu uživatel nebude moci spolehnout. Bezpečí při velkém počtu vychází z pravidla, že při tak velkém množství uživatelů Internetu je pravděpodobnost napadení velice malá. Na druhou stranu platí, že s rostoucí výkonností počítačů jeden člověk zvládne napadnout více počítačů za kratší dobu. Bezpečnostní pravidlo Bezpečí díky neznalosti vychází z toho, že spousta uživatelů nemá takové vzdělání, aby dokázala napadnout cizí počítač. Nutno ale říci, že s rozšířeností Internetu roste i vzdělání v tomto oboru.

8.3. Budoucnost šifrování

Ač šifrování bývá spolehlivým prostředkem poctivých uživatelů k ochraně jejich elektronických dat, stejnou službu poskytuje i zločincům, kteří svou komunikaci mezi sebou šifrují a tím policii a vládě znesnadňují dopadnutí. Proto vlády ve spoustě zemí usilují o zavedení zákona, který by jim umožnil získat pravomoci k neomezenému přístupu k takovým zprávám. Může se tedy počítat s rozšířením státních odposlechů elektronické komunikace.

Na druhou stranu by mohly být vytvořeny takové bezpečné šifrovací programy, které dokážou, že se nezjistí, že data někdo zašifroval, protože nebude vidět, že tam nějaká data jsou.

8.4. Narušování soukromí

V budoucnu bude na Internetu přes všechny opatření méně soukromí. Ti, co narušují soukromí, budou vždy o něco dál než jejich oběti se svými bezpečnostními opatřeními. V tomto případě však nedůvěra a opatrnost uživatelů roste a bude růst i dále. Lidé stále více chrání své osobní a citlivé údaje, protože jejich zneužití se začíná krutě nevyplácet.

8.5. Podvody

Počet různých podvodů se zvyšuje a jejich technické provedení se vylepšuje. Na druhou stranu všeobecné povědomí o různých druzích internetových podvodů se vždy po nějaké době zvýší natolik, že se pravděpodobnost, že se na ně ještě někdo nachytá, časem snižuje. Takové podvody zaniknout. Vzniknou ale nové druhy podvodů, které budou stále důmyslnější. Bude zase obtížné je odhalit – než se opět dostanou do všeobecného povědomí. Stále se budou k Internetu připojovat noví a nezkušení uživatelé, kteří se stanou obětí nějakého podvodníka. Proto je v zájmu každého uživatele, aby se co nejrychleji s prostředím Internetu seznámil, aby nemohl být lehce oklamán.

8.6. Trendy v obchodování po Internetu

Obchodování bude probíhat ve stále větší míře prostřednictvím Internetu a je těžko říci, jestli více bezpečně. Bude se však klást stále větší důraz na prokázání totožnosti, třeba prostřednictvím elektronického podpisu. Nejlepším řešením by pak bylo, aby elektronický podpis byl součástí prohlížeče Internetu, aby vše, co uživatel na Internetu udělá, mu mohlo být prokázáno. Výhody jsou zřejmé: jednak nebude možné uživateli prokázat, co na Internetu neudělal, a jednak bude možné dokázat, co je výsledkem jeho internetové činnosti.

Rizika spojená s obchodováním prostřednictvím Internetu mohou být snížena masovějším používáním webové kamery (např. živou ukázkou zboží i prodejce, předběžnou ústní dohodou apod.).

8.7. Spamming

Spamování se stále rozrůstá, přestože je v České republice od roku 2004 nelegální. Možná však firmy již brzy zjistí, že místo toho, aby svou reklamou zákazníky získali, je spíše odpuzují. Řešením tohoto problému mohou být nové a výkonnější prostředky pro odstraňování spamu v e-mailových klientech a dokonalé seznamy adres, ze kterých se rozesílá spam. Že spam příjemce okrádá o čas, peníze a strojové kapacity je věc známá. Může se ale stát, že míra spamu může v budoucnosti ohrozit elektronickou komunikaci natolik, že nebude použitelná.

8.8. Legislativa budoucnosti

Spousta oblastí Internetu potřebuje důslednou právní úpravu, ať už se jedná o elektronickou komunikaci uživatelů s úřady, telefonování po Internetu, rozhlasové a televizní vysílání přes Internet, elektronické obchodování atd.

Nejhorším a nejrozšířenějším neetickým (a vlastně i nelegálním) problémem Internetu se zdá být porušování autorského práva. Hlavními příčinami je jednoduchost provedení a mezi lidmi stále trvající vědomí, že „je-li něco na Internetu vystaveno široké veřejnosti, může se to neomezeně kopírovat a rozšiřovat“. Vzdělání a postihy občanů v této otázce jsou nedostatečné, přestože uživatelé tuší, že je to nesprávné, dokonce nezákonné.

Jedním z dalších největších problémů Internetu je zveřejňování nebezpečných informací, jako jsou např. podpora trestných a teroristických činů, propagace násilí, dětská pornografie apod. Dokud bude na Internetu poptávka po těchto materiálech, z Internetu nezmizí. V takových případech by se mělo postupovat jako v reálném životě: co je trestné ve skutečném světě, musí být trestné i na Internetu. Bylo by dobré, kdyby poskytovatelé připojení na Internet více sledovali obsah WWW stránek, které se na jejich serveru nachází.

V budoucnosti bude nutné se zabývat hlavně potlačování takových činů na Internetu jako jsou porušování autorských práv a propagace nebezpečných materiálů a myšlenek na webových stránkách. Dle mého názoru je nezbytné za tyto činy stanovit vysoké trestní sazby.

8.9. Závěry

S mírou uživatelského zabezpečení poroste počet rizik, která budou uživateli hrozit. Internet nepotřebuje přímo nové zákony, ve většině případů stačí přizpůsobit ty staré. V tomto prostředí se totiž neobjevuje nic nového, jen se to děje jinak, levněji, rychleji a efektivněji. Internet je ve svém vývoji nepředvídatelný, je tedy těžké říci, zda bude v budoucnosti na Internetu více cenzury a omezení či více svobody, a která z těchto dvou variant bude horší. To ukáže čas a hlavně praxe.

9. Závěr

Diplomová práce „Etika v prostředí Internetu“ pojednává o etickém a neetickém chování uživatelů v tomto virtuálním prostředí. Hlavní zásadou pro její vypracování bylo poskytnout celistvý pohled na tuto problematiku, tzn. definovat a rozpracovat pravidla pro etické chování na Internetu a naproti tomu popsat druhy neetického chování a poskytnout řešení a ochranu před tímto chováním, včetně platných českých zákonů, jejichž znění se dá aplikovat i na oblast Internetu.

Po úvodních slovech a stručné charakteristice sítě Internet čtenáře seznamuje s obecnými zásadami, kterými by se všichni uživatelé Internetu měli řídit, aby bylo dosaženo všeobecné spokojenosti při jeho používání a aby nikdo nebyl poškozen. Jedná se jakási pravidla ohleduplnosti k ostatním uživatelům. Obsahuje konkrétní pravidla, která byla před více jak 10 lety vytvořena zkušenými uživateli Internetu.

Práce pokračuje vymezením pravidel chování v konkrétních oblastech Internetu, jako je elektronická pošta, diskusní skupiny, FTP a WWW služba. Pravidla ve třetí a čtvrté kapitole více méně vycházejí z dokumentu RFC 1855 (viz přílohu č. 1), který zcela pokrývá mé potřeby pro splnění cíle o přehledu etických zásad chování uživatelů na Internetu.

Pátá kapitola je rozdělena na 4 podkapitoly (Soukromí, Vlastnictví, Svoboda, Morálka). Každá ze čtyř podkapitol představuje nějakou hodnotu uživatele Internetu, která může být neetickým chováním jiného uživatele ohrožena. Každá z těchto podkapitol potom obsahuje možné druhy hrozeb a způsoby, jak tuto hodnotu poškodit. Soukromí může být narušeno hackery a crackery, sběrem osobních dat uživatelů, porušením soukromí elektronické pošty, falšováním e-mailů, WWW stránek, diskusních příspěvků. Vlastnictví je ohroženo porušováním vlastnických práv, podvody, škodlivým softwarem, spamem nebo podvodným obchodováním. Svoboda uživatele je ohrožena cenzurou a regulací obsahu. Morálka je potom narušena neslušným chováním, prezentací problematických a nepravdivých informací na Internetu, změnou identity nebo neoprávněnou registrací doménového jména.

Cílem této kapitoly byl kompletní výčet problémů, se kterými se uživatel může při používání Internetu setkat, a jejich zařazení do správné kategorie. Problémy se vzájemně prolínají a jsou více i méně vážné. Představují situace, kdy je porušen zákon nebo alespoň všeobecně (i když ne legislativně) uznávaná etika Internetu. Základních etických problémů, se kterými se uživatel může setkat při používání Internetu, je 17, a tolik je i podkapitol v následující kapitole 6.

V šesté kapitole jsem si kladla za cíl najít řešení, jak se vyhnout, popřípadě čelit problémům uvedeným v kapitole pět. U každého problému jsou vypsány rady, postupy, příslušné programy, mechanismy a návody, které pomohou ochránit uživatele před neetickým chováním ostatních uživatelů a pachatelů trestních činů na Internetu. Rady jsou jak preventivní, tak obranné. Dalším cílem bylo naleznout ke každému problému odpovídající legislativu, která by taktéž měla chránit práva uživatelů.

Mým dalším cílem bylo rozlišit internetové hrozby na ty, které uživateli skutečně při používání Internetu hrozí a na ty, u nichž není příliš pravděpodobné, že se s nimi uživatel setká. Dále jsem považovala za důležité rozlišit internetové útoky dle nebezpečnosti – od těch, které jsou bezvýznamné až po ty, které jsou skutečně nebezpečné. Tyto otázky řeší sedmá kapitola.

Etika a hlavně neetika páchaná na Internetu patří k aktuálním tématům dnešní doby. S Internetem se denně setkává spousta lidí, mnoho lidí ho využívá a potřebuje ke své práci i zábavě. Ale počítač připojený k Internetu může vždy znamenat nebezpečí. S tímto tvrzením souvisí fakt, že s přibývajícím počtem uživatelů Internetu roste také počet soudních sporů v této oblasti. Přičemž vypátrat člověka, který prostřednictvím Internetu škodí, je velice těžké.

Vnímání hranice mezi tím, co je ještě etické, a tím, co už není, je u každého člověka individuální. Ale celkově vzato lidé vědí, kam už zajít nemohou. Leč někteří to vědí a stejně tyto hranice překračují. Rozhodně to neznamená, že by se člověk měl pro strach ze špiónů, crackerů a podvodníků bát využívat krás a výhod Internetu. Ale rozhodně by se měl průběžně informovat o bezpečnosti na Internetu a sledovat aktuální hrozby a možnosti, jak se jim vyhnout a jak se před nimi chránit.

Diplomová práce je přínosem jednak v komplexním pohledu na tuto problematiku, pak v rozdělení internetového chování na etické a neetické, v analýze obou druhů chování, a v rámci neetiky pak výčtem různých případů neetického chování. Za přínosné dále považuji počet nalezených opatření a řešení neetiky na Internetu, a hlavně vyhledání legislativy, která se ke konkrétním situacím vztahuje.

Hlavní i dílčí cíle mé práce jsem splnila. Snažila jsem se o vyčerpávající výčet etických zásad i neetických problémů na Internetu a poskytla jsem různé řešení situací pro uživatele, který se s daným problémem setká. Myslím, že všechny nalezené postupy včetně legislativy odpovídají praxi a jsou užitečné pro každého, kdo Internet používá.

Slovníček pojmů

Adware	Software přidávající do programů reklamu.
Anonymizér	Program umožňující skrýt identitu uživatele při prohlížení WWW stránek.
Antispam	Systém, který se snaží identifikovat a popřípadě i zničit spam.
Antispyware	Program na detekování a ničení spywaru.
Antivir	Antivirový program. Program pro vyhledávání a ničení počítačových virů.
Asymetrické šifrování	Šifrování s veřejným klíčem.
Autorské právo, copyright	Typ právní ochrany duševního vlastnictví.
Banner	Forma internetové reklamy.
Blacklist	Seznam IP adres, které jsou falšované nebo je z nich odesílán spam.
Cenzura	Druh omezení nebo regulace.
Cookie	Textový soubor, který pro provozovatele webových stránek sbírá demografické a jiné informace.
Copyboarding	Totální zákaz kopírování díla.
Copylefting	GNU General Public License, možnost volného používání a šíření kódu programu pod značkou GPL.
Cracker	Zákeřný člověk vnikající do počítačů jiných uživatelů pomocí nedostatků v zabezpečení systému.
Crossposting	Rozesílání stejného příspěvku do různých diskusí, což u ostatních uživatelů vede k obdržení několika kopií téhož příspěvku.
Cybersquatting	Ukradení názvu atraktivní domény.
Demoware	Volně šiřitelný software, který je limitovanou verzí placeného programu.
Dialer	Program, který dokáže změnit způsob přístupu na Internet.
DNS Blacklist	Seznam falšovaných IP adres.
Etické kodexy, etika	Systém morálních principů a pravidel chování.
Firewall	Soubor opatření (HW a SW), která zabezpečují síť proti neoprávněnému přístupu zvenčí a proti úniku informací.
Flamewar	Vášnivá diskuse na Internetu.
Freeware	Zdarma šiřitelný program.

Google bomba	Zneužití funkce vyhledávače vedoucí většinou k zesměšnění nějaké osoby či skupiny osob.
Graylisting	Funkce bojující se spamem využívající opětovného doručení.
Hacker	Dříve znamenal schopného uživatele počítače a programátora, v současnosti počítačového piráta.
Hoax	Poplašná zpráva šířená prostřednictvím Internetu.
Instant Messaging	Internetová služba interaktivní komunikace.
Internet	Celosvětová síť spojující menší sítě pomocí protokolů IP.
Keylogger	Špionážní program, který zaznamenává stisknuté klávesy, kliknutí myší, snímá obrazovku apod.
Licensing	Distribuce softwaru založená na dodržování licenčních podmínek.
Lock program	Program blokující klávesnici a myš.
Mailbombing	Bombardování uživatele velkým množstvím zpráv.
Malware	Škodlivý software (počítačové viry, červy, trojské koně atd.)
Netiketa, síťová etika	Pravidla chování v počítačové síti (např. na Internetu).
Nick	Přezdívka.
Pharming	Přesměrování uživatele na falešnou IP adresu s cílem vylákat z něj citlivé údaje.
Phishing	E-mail, který nabádá k připojení uživatele na podvržené WWW stránky s cílem vylákat z něj citlivé údaje.
Počítačový vir	Škodlivý software. Části počítačového kódu, které dokážou infikovat a poškodit data v počítači.
Počítačový červ	Škodlivý software přebírající kontrolu nad počítačem.
Public domain	Software určený pro veřejné použití.
Remailer	Služba, která umožňuje přijímat a odesílat e-maily anonymně.
RFC 1855	Soubor pravidel síťové netikety.
Scam, scammer	Podvod, podvodník.
Shareware	Za malý poplatek distribuovaný software, nezbavený autorských práv.
Sociotechnika (sociální inženýrství)	Ovlivňování lidí s cílem oklamat je a získat od nich např. tajné informace.
Spamování, spamming	Rozesílání nevyžádané pošty, většinou reklamního charakteru.
Spyware	Skrytý program v počítači uživatele, který odesílá důvěrné informace třetím osobám.
Symetrické šifrování	Šifrování se soukromým klíčem.

Telnet	Telecommunicatons Network. Protokol TCP umožňující připojení ke vzdálené stanici či uzlu.
Transference	Činnost mozku, který si sám doplní chybějící informace.
Trojský kůň	Škodlivý program obsahující vir, nechtěnou funkci apod.
Troll	Člověk, který se snaží vyvolat u jiných lidí negativní emoce, nebo výsledek jeho snažení (např. zesměšnění jiného uživatele).
Wetware	Lidská nervová soustava.
Whitelist	IP adresy odesílající legitimní zprávy.

Seznam použité literatury a zdrojů

[1] PAVLOVSKÝ, R., SKLENÁK, V. *Informace a Internet.* 1. vyd. Praha: Vysoká škola ekonomická, 1998. ISBN 80-7079-562-X.

[2] SMEJKAL, V. *Internet a paragrafy.* 1. vyd. Praha: Grada Publishing, s. r. o., 2001. ISBN 80-7169-765-6.

[3] BARRETT, D. J. *Bandits on the Information Superhighway.* 1st ed., Cambridge: O´ Really & Associates, Inc., 1996. ISBN 1-56592-156-9.

[4] CEJPEK, J. *Informace, komunikace a myšlení.* 1. vyd. Praha: Karolinum, 2005. ISBN 80-7184-767-4.

[5] SHEA, V. *The Core Rules of Netiquette* [online]. [cit. 16. 6. 2007]. Dostupné z: http://www.albion.com /netiquette/corerules.html

[6] STŘIHAVKA, M. *Vaše bezpečnost a anonymita na Internetu.* 1. vyd. Praha: Computerpress, 2001. ISBN 80-7226-586-5.

[7] *Wikipedie, otevřená encyklopedie* [online]. [cit. 31. 10. 2007]. Dostupné z: http://cs.wikipedia.org/wiki/Fair_use

[8] HÖSCHL, C. Očima C. H. *Reflex.* Praha: 2007, roč. 18, č. 42, s. 23. ISSN 0862-6634.

[9] *RFC 1855, Netiquette Guidelines* [online]. [cit. 2. 11. 2007]. Dostupné z: http://www.dtcc.edu/cs/rfc1855.html

[10] *Ochrana duševního vlastnictví* [online]. [cit. 8. 11. 2007]. Dostupné z: www.komora.cz/DownloadHandler.aspx?method=GetFileDownload&fileID=258&DontParse=true

[11] *Petr Kolář: Operační systém Unix* [online]. [cit. 15. 11. 2007]. Dostupné z: http://www.kit.vslib.cz/~kolar/unix/oldhtml/

[12] BEDRNOVÁ, J. Chat: jsi kluk, nebo holka? *Mladá fronta Plus.* Praha: 2007, roč. 5, č. 36, s. 52. ISSN 1214-4746.

[13] *Wikipedie, otevřená encyklopedie* [online]. [cit. 6. 10. 2007]. Dostupné z: http://cs.wikipedia.org/wiki/Copyright

[14] SMEJKAL, V., aj. *Právo informačních a telekomunikačních systémů.* 1. vyd. Praha: C. H. Beck, 2001. ISBN 80-7179-522-6.

[15] *Listina základních práv a svobod (Ústavní zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1993 Sb.)* [online]. [cit. 4. 11. 2007]. Dostupné z: http://www.psp.cz/docs/laws/listina.html

[16] *Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů* [online]. [cit. 4. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/obcanzak/

[17] *Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů* [online]. [cit. 4. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/

[18] *Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů* [online]. [cit. 4. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/zivnost/

[19] *Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů* [online]. [cit. 4. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/spravni_rad/

[20] *Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů* [online]. [cit. 4. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/trestni_zakon/

[21] *Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/trestni_rad/

[22] *Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/osr/

[23] *Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/prestupky/

[24] *Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/autorsky/

[25] *Zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.e-law.cz/zakony/151_2000.txt

[26] *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/epodpis/

[27] *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/oou/

[28] *Zákon č. 137/1995 Sb., o ochranných známkách, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.e-law.cz/zakony/137_95.txt

[29] *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.nbu.cz/legislativa/412_2005.php

[30] *Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.nbu.cz/legislativa/412_2005.php

[31] *Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.lexdata.cz/lexdata/sb_free.nsf/

[32] *Zákon č. 478/1992 Sb., o užitných vzorech, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.e-law.cz/zakony/478_92.txt

[33] *Zákon č. 256/1992 Sb.,o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.lexdata.cz/lexdata/sb_free.nsf/

[34] *Zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.mvcr.cz/dokument/2006/283_1991.pdf

[35] *Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.lexdata.cz/lexdata/sb_free.nsf/

[36] *Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/banky/

[37] *Zákon č. 154/1994 Sb., o Bezpečnostní informační službě* [online]. [cit. 18. 11. 2007]. Dostupné z: http://portal.gov.cz/wps/portal/_s.155/701?kam=zakon&c=154/1994

[38] *Zákon č. 552/1991 Sb., o státní kontrole* [online]. [cit. 18. 11. 2007]. Dostupné z: http://portal.gov.cz/wps/portal/_s.155/701?kam=zakon&c=552/1991

[39] *Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb98148&cd=76&typ=r

[40] *Zákon č. 29/2000, o poštovních službách a o změně některých zákonů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00029&cd=76&typ=r

[41] *Zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.digizone.cz/zakony/zakon-40-1995/

[42] *Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://business.center.cz/business/pravo/zakony/spotrebitel/

[43] *Zákon č. 268/1949 Sb., o matrikách, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.lexdata.cz/lexdata/sb_free.nsf/

[44] *Zákon č. 55/1950 Sb., o užívání a změně jména a příjmení, ve znění pozdějších předpisů* [online]. [cit. 18. 11. 2007]. Dostupné z: http://www.lexdata.cz/lexdata/sb_free.nsf/

[45] *Směrnice Rady 85/577/EHS ze dne 20. prosince 1985, o ochraně spotřebitele v případě smluv uzavřených mimo obchodní prostory* [online]. [cit. 28. 11. 2007]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0577:CS:HTML

[46] *Smernica Rady 91/250/EHS zo 14. mája 1991, o právnej ochrane počítačových programov* [online]. [cit. 28. 11. 2007]. Dostupné z: http://www.culture.gov.sk/files/files/copyright/91_250_EHSsvk.pdf

[47] *Směrnice Rady 93/13/EHS ze dne 5. dubna 1993, o nepřiměřených podmínkách ve spotřebitelských smlouvách* [online]. [cit. 28. 11. 2007]. Dostupné z: http://www.mdcr.cz/NR/rdonlyres/

[48] *Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.* [online]. [cit. 28. 11. 2007]. Dostupné z: http://eur-ex.europa.eu/LexUriServ/site/cs/dd/13/15/31995L0046CS.pdf

[49] *Směrnice Evropského parlamentu a Rady 97/7/ES ze dne 20. května 1997, o ochraně spotřebitele v případě smluv uzavřených na dálku* [online]. [cit. 28. 11. 2007]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:CS:HTML

[50] *Smernica Európskeho parlamentu a Rady 97/66/ES z 15. decembra 1997, o spracovaní osobných údajov a ochrane súkromia v telekomunikačnom sektore* [online]. [cit. 28. 11. 2007]. Dostupné z: http://www.telecom.gov.sk/externe/legeu/telekom/97-0066.pdf

[51] *Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999, o zásadách Společenství pro elektronické podpisy* [online]. [cit. 28. 11. 2007]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:CS:HTML

[52] *Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých práv. aspektech služeb inform. společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu)* [online]. [cit. 28. 11. 2007]. Dostupné z: http://eur -lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:CS:HTML

[53] *Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001, o harmonizaci některých aspektů autorského práva a práv s ním souvisejících v informační*

společnosti [online]. [cit. 28. 11. 2007]. Dostupné z: http://www.nkp.cz/o_knihovnach/AutZak/smernice.RTF

[54] *Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)* [online]. [cit. 28. 11. 2007]. Dostupné http://www.micr.cz/images/dokumenty/32002L0058.pdf

[55] *Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES* [online]. [cit. 28. 11. 2007]. Dostupné http://eur-lex.europa.eu/LexUriServ/site/cs/oj/2006/l_105/l_10520060413cs00540063.pdf

[56] *Bernská úmluva o ochraně literárních a uměleckých děl ze dne 9. září 1886, ve znění pozdějších změn a doplňků* [online]. [cit. 28. 11. 2007]. Dostupné z: http://cs.wikisource.org/wiki/Bernská úmluva o ochraně literárních a uměleckých děl

[57] *The Universal Copyright Convention (Geneva Text – September 6, 1952)* [online]. [cit. 28. 11. 2007]. Dostupné z: http://ipmall.info/hosted_resources/lipa/copyrights/The%20Universal%20Copyright%20Convention%20_Geneva%20Text--September.pdf

[58] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28. I. 1981* [online]. [cit. 28. 11. 2007]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Seznam obrázků, grafů a tabulek

Seznam příloh

Příloha č. 1:

Vybrané části z dokumentu RFC 1855 (Pokyny pro netiketu)

Status of This Memo
This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract
This document provides a minimum set of guidelines for Network Etiquette (Netiquette) which organizations may take and adapt for their own use. As such, it is deliberately written in a bulleted format to make adaptation easier and to make any particular item easy (or easier) to find. It also functions as a minimum set of guidelines for individuals, both users and administrators. This memo is the product of the Responsible Use of the Network (RUN) Working Group of the IETF.

1.0 Introduction
In the past, the population of people using the Internet had "grown up" with the Internet, was technically minded, and understood the nature of the transport and the protocols. Today, the community of Internet users includes people who are new to the environment. These "Newbies" are unfamiliar with the culture and don't need to know about transport and protocols. In order to bring these new users into the Internet culture quickly, this Guide offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use. Individuals should be aware that no matter who supplies their Internet access, be it an Internet Service Provider through a private account, or a student account at a University, or an account through a corporation, that those organizations have regulations about ownership of mail and files, about what is proper to post or send, and how to present yourself. Be sure to check with the local authority for specific guidelines.

We've organized this material into three sections: One-to-one communication, which includes mail and talk; One-to-many communications, which includes mailing lists and NetNews; and Information Services, which includes ftp, WWW, Wais, Gopher, MUDs and MOOs. Finally, we have a Selected Bibliography, which may be used for reference.

2.0 One-to-One Communication (electronic mail, talk)
We define one-to-one communications as those in which a person is communicating with another person as if face-to-face: a dialog. In general, rules of common courtesy for interaction with people should be in force for any situation and on the Internet it's doubly important where, for example, body language and tone of voice must be inferred.

2.1 User Guidelines

2.1.1 For mail:

- Unless you have your own Internet access through an Internet provider, be sure to check with your employer about ownership of electronic mail. Laws about the ownership of electronic mail vary from place to place.
- Unless you are using an encryption device (hardware or software), you should assume that mail on the Internet is not secure. Never put in a mail message anything you would not put on a postcard.
- Respect the copyright on material that you reproduce. Almost every country has copyright laws.
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are re-posting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.

- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator if your ever receive one.
- A good rule of thumb: Be conservative in what you send and liberal in what you receive. You should not send heated messages (we call these "flames") even if you are provoked. On the other hand, you shouldn't be surprised if you get flamed and it's prudent not to respond to flames.
- In general, it's a good idea to at least check all your mail subjects before responding to a message. Sometimes a person who asks you for help (or clarification) will send another message which effectively says "Never Mind". Also make sure that any message you respond to was directed to you. You might be cc:ed rather than the primary recipient.
- Make things easy for the recipient. Many mailers strip header information which includes your return address. In order to ensure that people know who you are, be sure to include a line or two at the end of your message with contact information. You can create this file ahead of time and add it to the end of your messages. (Some mailers do this automatically.) In Internet parlance, this is known as a ".sig" or "signature" file. Your .sig file takes the place of your business card. (And you can have more than one to apply in different circumstances.)
- Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending.
- Watch cc's when replying. Don't continue to include people if the messages have become a 2-way conversation.
- In general, most people who use the Internet don't have time to answer general questions about the Internet and its workings. Don't send unsolicited mail asking for information to people whose names you might have seen in RFCs or on mailing lists.
- Remember that people with whom you communicate are located across the globe. If you send a message to which you want an immediate response, the person receiving it might be at home asleep when it arrives. Give them a chance to wake up, come to work, and login before assuming the mail didn't arrive or that they don't care.
- Verify all addresses before initiating long or personal discourse. It's also a good practice to include the word "Long" in the subject header so the recipient knows the message will take time to read and respond to. Over 100 lines are considered "long".
- Know whom to contact for help. Usually you will have resources close at hand. Check locally for people who can help you with software and system problems. Also, know whom to go to if you receive anything questionable or illegal. Most sites also have "Postmaster" aliased to a knowledgeable user, so you can send mail to this address to get help with mail.
- Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. Be especially careful with sarcasm.
- Use mixed case. UPPER CASE LOOKS AS IF YOU'RE SHOUTING.
- Use symbols for emphasis. That *is* what I meant. Use underscores for underlining. _War and Peace_ is my favorite book.
- Use smiles to indicate tone of voice, but use them sparingly. :-) is an example of a smiley (Look sideways). Don't assume that the inclusion of a smiley will make the recipient happy with what you say or wipe out an otherwise insulting comment.
- Wait overnight to send emotional responses to messages. If you have really strong feelings about a subject, indicate it via FLAME ON/OFF enclosures. For example:
  FLAME ON:
  This type of argument is not worth the bandwidth it takes to send it. It's illogical and poorly reasoned.
  The rest of the world agrees with me.
  FLAME OFF
- Do not include control characters or non-ASCII attachments in messages unless they are MIME attachments or unless your mailer encodes these. If you send encoded messages make sure the recipient can decode them.
- Be brief without being overly terse. When replying to a message, include enough original material to be understood but no more. It is extremely bad form to simply reply to a message by including the entire previous message: edit out all the irrelevant material.
- Limit line length to fewer than 65 characters and end a line with a carriage return.
- Mail should have a subject heading which reflects the content of the message.

- If you include a signature keep it short. Rule of thumb is no longer than 4 lines. Remember that many people pay for connectivity by the minute, and the longer your message is, the more they pay.
- Just as mail (today) may not be private, mail (and news) is (today) subject to forgery and spoofing of various degrees of detects ability. Apply common sense "reality checks" before assuming a message is valid.
- If you think the importance of a message justifies it, immediately reply briefly to an e-mail message to let the sender know you got it, even if you will send a longer reply later.
- "Reasonable" expectations for conduct via e-mail depend on your relationship to a person and the context of the communication. Norms learned in a particular e-mail environment may not apply in general to your e-mail communication with people across the Internet. Be careful with slang or local acronyms.
- The cost of delivering an e-mail message is, on the average, paid about equally by the sender and the recipient (or their organizations). This is unlike other media such as physical mail, telephone, TV, or radio. Sending someone mail may also cost them in other specific ways like network bandwidth, disk space or CPU usage. This is a fundamental economic reason why unsolicited e-mail advertising is unwelcome (and is forbidden in many contexts).
- Know how large a message you are sending. Including large files such as Postscript files or programs may make your message so large that it cannot be delivered or at least consumes excessive resources. A good rule of thumb would be not to send a file larger than 50 Kilobytes. Consider file transfer as an alternative, or cutting the file into smaller chunks and sending each as a separate message.
- Don't send large amounts of unsolicited information to people.
- If your mail system allows you to forward mail, beware the dreaded forwarding loop. Be sure you haven't set up forwarding on several hosts so that a message sent to you gets into an endless loop from one computer to the next to the next.

2.1.2 For talk:

Talk is a set of protocols which allow two people to have an interactive dialogue via computer.

- Use mixed case and proper punctuation, as though you were typing a letter or sending mail.
- Don't run off the end of a line and simply let the terminal wrap; use a Carriage Return (CR) at the end of the line. Also, don't assume your screen size is the same as everyone else's. A good rule of thumb is to write out no more than 70 characters and no more than 12 lines (since you're using a split screen).
- Leave some margin; don't write to the edge of the screen.
- Use two CRs to indicate that you are done and the other person may start typing. (blank line).
- Always say goodbye, or some other farewell, and wait to see a farewell from the other person before killing the session. This is especially important when you are communicating with someone a long way away. Remember that your communication relies on both bandwidth (the size of the pipe) and latency (the speed of light).
- Remember that talk is an interruption to the other person. Only use as appropriate. And never talk to strangers.
- The reasons for not getting a reply are many. Don't assume that everything is working correctly. Not all versions of talk are compatible.
- If left on its own, talk re-rings the recipient. Let it ring one or two times, then kill it.
- If a person doesn't respond you might try another TTY. Use finger to determine which are open. If the person still doesn't respond, do not continue to send.
- Talk shows your typing ability. If you type slowly and make mistakes when typing it is often not worth the time of trying to correct, as the other person can usually see what you meant.
- Be careful if you have more than one talk session going!

2.2 Administrator Issues

- Be sure you have established written guidelines for dealing with situations especially illegal, improper, or forged traffic.
- Handle requests in a timely fashion - by the next business day.

- Respond promptly to people who have concerns about receiving improper or illegal messages. Requests concerning chain letters should be handled immediately.
- Explain any system rules, such as disk quotas, to your users. Make sure they understand implications of requesting files by mail such as: Filling up disks; running up phone bills, delaying mail, etc.
- Make sure you have "Postmaster" aliased. Make sure you have "Root" aliased. Make sure someone reads that mail.
- Investigate complaints about your users with an open mind. Remember that addresses may be forged and spoofed.

3.0 One-to-Many Communication (Mailing Lists, NetNews)

Any time you engage in One-to-Many communications, all the rules for mail should also apply. After all, communicating with many people via one mail message or post is quite analogous to communicating with one person with the exception of possibly offending a great many more people than in one-to-one communication. Therefore, it's quite important to know as much as you can about the audience of your message.

3.1 User Guidelines

3.1.1 General Guidelines for mailing lists and NetNews

- Read both mailing lists and newsgroups for one to two months before you post anything. This helps you to get an understanding of the culture of the group.
- Do not blame the system administrator for the behavior of the system users.
- Consider that a large audience will see your posts. That may include your present or your next boss. Take care in what you write. Remember too, that mailing lists and Newsgroups are frequently archived, and that your words may be stored for a very long time in a place to which many people have access.
- Assume that individuals speak for themselves, and what they say does not represent their organization (unless stated explicitly).
- Remember that both mail and news take system resources. Pay attention to any specific rules covering their uses your organization may have.
- Messages and articles should be brief and to the point. Don't wander off-topic, don't ramble and don't send mail or post messages solely to point out other people's errors in typing or spelling. These, more than any other behavior, mark you as an immature beginner.
- Subject lines should follow the conventions of the group.
- Forgeries and spoofing are not approved behavior.
- Advertising is welcomed on some lists and Newsgroups, and abhorred on others! This is another example of knowing your audience before you post. Unsolicited advertising which is completely off-topic will most certainly guarantee that you get a lot of hate mail.
- If you are sending a reply to a message or a posting be sure you summarize the original at the top of the message, or include just enough text of the original to give a context. This will make sure readers understand when they start to read your response. Since NetNews, especially, is proliferated by distributing the postings from one host to another, it is possible to see a response to a message before seeing the original. Giving context helps everyone. But do not include the entire original!
- Again, be sure to have a signature which you attach to your message. This will guarantee that any peculiarities of mailers or newsreaders which strip header information will not delete the only reference in the message of how people may reach you.
- Be careful when you reply to messages or postings. Frequently replies are sent back to the address which originated the post - which in many cases is the address of a list or group! You may accidentally send a personal response to a great many people, embarrassing all involved. It's best to type in the address instead of relying on "reply."
- Delivery receipts, non-delivery notices, and vacation programs are neither totally standardized nor totally reliable across the range of systems connected to Internet mail. They are invasive when sent to mailing lists, and some people consider delivery receipts an invasion of privacy. In short, do not use them.

- If you find a personal message has gone to a list or group, send an apology to the person and to the group.
- If you should find yourself in a disagreement with one person, make your responses to each other via mail rather than continue to send messages to the list or the group. If you are debating a point on which the group might have some interest, you may summarize for them later.
- Don't get involved in flame wars. Neither post nor respond to incendiary material.
- Avoid sending messages or posting articles which are no more than gratuitous replies to replies.
- Be careful with monospacing fonts and diagrams. These will display differently on different systems, and with different mailers on the same system.
- There are Newsgroups and Mailing Lists which discuss topics of wide varieties of interests. These represent a diversity of lifestyles, religions, and cultures. Posting articles or sending messages to a group whose point of view is offensive to you simply to tell them they are offensive is not acceptable. Sexually and racially harassing messages may also have legal implications. There is software available to filter items you might find objectionable.

3.1.2 Mailing List Guidelines

There are several ways to find information about what mailing lists exist on the Internet and how to join them. Make sure you understand your organization's policy about joining these lists and posting to them. In general it is always better to check local resources first before trying to find information via the Internet. Nevertheless, there are a set of files posted periodically to news.answers which list the Internet mailing lists and how to subscribe to them. This is an invaluable resource for finding lists on any topic.

- Send subscribe and unsubscribe messages to the appropriate address. Although some mailing list software is smart enough to catch these, not all can ferret these out. It is your responsibility to learn how the lists work, and to send the correct mail to the correct place. Although many many mailing lists adhere to the convention of having a "-request" alias for sending subscribe and unsubscribe messages, not all do. Be sure you know the conventions used by the lists to which you subscribe.
- Save the subscription messages for any lists you join. These usually tell you how to unsubscribe as well.
- In general, it's not possible to retrieve messages once you have sent them. Even your system administrator will not be able to get a message back once you have sent it. This means you must make sure you really want the message to go as you have written it.
- The auto-reply feature of many mailers is useful for in-house communication, but quite annoying when sent to entire mailing lists. Examine "Reply-To" addresses when replying to messages from lists. Most auto-replies will go to all members of the list.
- Don't send large files to mailing lists when Uniform Resource Locators (URLs) or pointers to ftp-able versions will do. If you want to send it as multiple files, be sure to follow the culture of the group. If you don't know what that is, ask.
- Consider unsubscribing or setting a "nomail" option (when it's available) when you cannot check your mail for an extended period.
- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting.
- If you ask a question, be sure to post a summary. When doing so, truly summarize rather than send a cumulation of the messages you receive.
- Some mailing lists are private. Do not send mail to these lists uninvited. Do not report mail from these lists to a wider audience.
- If you are caught in an argument, keep the discussion focused on issues rather than the personalities involved.

3.1.3 NetNews Guidelines

NetNews is a globally distributed system which allows people to communicate on topics of specific interest. It is divided into hierarchies, with the major divisions being: sci - science related discussions; comp - computer related discussions; news - for discussions which center around NetNews itself; rec - recreational activities; soc - social issues; talk - long-winded never-ending discussions; biz - business related postings; and alt - the alternate hierarchy. Alt is so named because creating an alt group does not go through the same process as creating a group in the other parts of the hierarchy. There are also regional hierarchies, hierarchies

which are widely distributed such as Bionet, and your place of business may have its own groups as well. Recently, a "humanities" hierarchy was added, and as time goes on its likely more will be added.

- In NetNews parlance, "Posting" refers to posting a new article to a group, or responding to a post someone else has posted. "Cross-Posting" refers to posting a message to more than one group. If you introduce Cross-Posting to a group, or if you direct "Followup-To:" in the header of your posting, warn readers! Readers will usually assume that the message was posted to a specific group and that followups will go to that group. Headers change this behavior.
- Read all of a discussion in progress (we call this a thread) before posting replies. Avoid posting "Me Too" messages, where content is limited to agreement with previous posts. Content of a follow-up post should exceed quoted content.
- Send mail when an answer to a question is for one person only. Remember that News has global distribution and the whole world probably is NOT interested in a personal response. However, don't hesitate to post when something will be of general interest to the Newsgroup participants.
- Check the "Distribution" section of the header, but don't depend on it. Due to the complex method by which News is delivered, Distribution headers are unreliable. But, if you are posting something which will be of interest to a limited number or readers, use a distribution line that attempts to limit the distribution of your article to those people. For example, set the Distribution to be "nj" if you are posting an article that will be of interest only to New Jersey readers.
- If you feel an article will be of interest to more than one Newsgroup, be sure to CROSSPOST the article rather than individually post it to those groups. In general, probably only five-to-six groups will have similar enough interests to warrant this.
- Consider using Reference sources (Computer Manuals, Newspapers, help files) before posting a question. Asking a Newsgroup where answers are readily available elsewhere generates grumpy "RTFM" (read the fine manual - although a more vulgar meaning of the word beginning with "f" is usually implied) messages.
- Although there are Newsgroups which welcome advertising, in general it is considered nothing less than criminal to advertise off-topic products. Sending an advertisement to each and every group will pretty much guarantee your loss of connectivity.
- If you discover an error in your post, cancel it as soon as possible.
- DO NOT attempt to cancel any articles but your own. Contact your administrator if you don't know how to cancel your post, or if some other post, such as a chain letter, needs canceling.
- If you've posted something and don't see it immediately, don't assume it's failed and re-post it.
- Some groups permit (and some welcome) posts which in other circumstances would be considered to be in questionable taste. Still, there is no guarantee that all people reading the group will appreciate the material as much as you do. Use the Rotate utility (which rotates all the characters in your post by 13 positions in the alphabet) to avoid giving offense. The Rot13 utility for Unix is an example.
- In groups which discuss movies or books it is considered essential to mark posts which disclose significant content as "Spoilers". Put this word in your Subject: line. You may add blank lines to the beginning of your post to keep content out of sight, or you may Rotate it.
- Forging of news articles is generally censured. You can protect yourself from forgeries by using software which generates a manipulation detection "fingerprint", such as PGP (in the US).
- Postings via anonymous servers are accepted in some Newsgroups and disliked in others. Material which is inappropriate when posted under one's own name is still inappropriate when posted anonymously.
- Expect a slight delay in seeing your post when posting to a moderated group. The moderator may change your subject line to have your post conform to a particular thread.
- Don't get involved in flame wars. Neither post nor respond to incendiary material.

3.2 Administrator Guidelines

3.2.1 General Issues

- Clarify any policies your site has regarding its subscription to NetNews groups and about subscribing to mailing lists.

- Clarify any policies your site has about posting to NetNews groups or to mailing lists, including use of disclaimers in .sigs.
- Clarify and publicize archive policy. (How long are articles kept?)
- Investigate accusations about your users promptly and with an open mind.
- Be sure to monitor the health of your system.
- Consider how long to archive system logs, and publicize your policy on logging.

3.2.2 Mailing Lists

- Keep mailing lists up to date to avoid the "bouncing mail" problem.
- Help list owners when problems arise.
- Inform list owners of any maintenance windows or planned downtime.
- Be sure to have "-request" aliases for list subscription and administration.
- Make sure all mail gateways operate smoothly.

3.2.3. NetNews

- Publicize the nature of the feed you receive. If you do not get a full feed, people may want to know why not.
- Be aware that the multiplicity of News Reader clients may cause the News Server being blamed for problems in the clients.
- Honor requests from users immediately if they request cancellation of their own posts or invalid posts, such as chain letters.
- Have "Usenet", "Netnews" and "News" aliased and make sure someone reads the mail.

3.3 Moderator Guidelines

3.3.1 General Guidelines

- Make sure your Frequently Asked Questions (FAQ) is posted at regular intervals. Include your guidelines for articles/messages. If you are not the FAQ maintainer, make sure they do so.
- Make sure you maintain a good welcome message, which contains subscribe and unsubscribe information.
- Newsgroups should have their charter/guidelines posted regularly.
- Keep mailing lists and Newsgroups up to date. Post messages in a timely fashion. Designate a substitute when you go on vacation or out of town.

4.0 Information Services (Gopher, Wais, WWW, ftp, telnet)

In recent Internet history, the 'Net has exploded with new and varied Information services. Gopher, Wais, World Wide Web (WWW), Multi-User Dimensions (MUDs) Multi-User Dimensions which are Object Oriented (MOOs) are a few of these new areas. Although the ability to find information is exploding, "Caveat Emptor" remains constant.

4.1 User Guidelines

4.1.1. General guidelines

- Remember that all these services belong to someone else. The people who pay the bills get to make the rules governing usage. Information may be free - or it may not be! Be sure you check.
- If you have problems with any form of information service, start problem solving by checking locally: Check file configurations, software setup, network connections, etc. Do this before assuming the problem is at the provider's end and/or is the provider's fault.
- Although there are naming conventions for file-types used, don't depend on these file naming conventions to be enforced. For example, a ".doc" file is not always a Word file.
- Information services also use conventions, such as www.xyz.com. While it is useful to know these conventions, again, don't necessarily rely on them.

- Know how file names work on your own system.
- Be aware of conventions used for providing information during sessions. FTP sites usually have files named README in a top level directory which have information about the files available. But, don't assume that these files are necessarily up-to-date and/or accurate.
- Do NOT assume that ANY information you find is up-to-date and/or accurate. Remember that new technologies allow just about anyone to be a publisher, but not all people have discovered the responsibilities which accompany publishing.
- Remember that unless you are sure that security and authentication technology is in use, that any information you submit to a system is being transmitted over the Internet "in the clear", with no protection from "sniffers" or forgers.
- Since the Internet spans the globe, remember that Information Services might reflect culture and life-style markedly different from your own community. Materials you find offensive may originate in a geography which finds them acceptable. Keep an open mind.
- When wanting information from a popular server, be sure to use a mirror server that's close if a list is provided.
- Do not use someone else's FTP site to deposit materials you wish other people to pick up. This is called "dumping" and is not generally acceptable behavior.
- When you have trouble with a site and ask for help, be sure to provide as much information as possible in order to help debug the problem.
- When bringing up your own information service, such as a homepage, be sure to check with your local system administrator to find what the local guidelines are in affect.
- Consider spreading out the system load on popular sites by avoiding "rush hour" and logging in during off-peak times.

4.1.2 Real Time Interactive Services Guidelines (MUDs MOOs IRC)

- As in other environments, it is wise to "listen" first to get to know the culture of the group.
- It's not necessary to greet everyone on a channel or room personally. Usually one "Hello" or the equivalent is enough. Using the automation features of your client to greet people is not acceptable behavior.
- Warn the participants if you intend to ship large quantities of information. If all consent to receiving it, you may send, but sending unwanted information without a warning is considered bad form just as it is in mail.
- Don't assume that people who you don't know will want to talk to you. If you feel compelled to send private messages to people you don't know, then be willing to accept gracefully the fact that they might be busy or simply not want to chat with you.
- Respect the guidelines of the group. Look for introductory materials for the group. These may be on a related ftp site.
- Don't badger other users for personal information such as sex, age, or location. After you have built an acquaintance with another user, these questions may be more appropriate, but many people hesitate to give this information to people with whom they are not familiar.
- If a user is using a nickname alias or pseudonym, respect that user's desire for anonymity. Even if you and that person are close friends, it is more courteous to use his nickname. Do not use that person's real name online without permission.

4.2 Administrator Guidelines

4.2.1 General Guidelines

- Make clear what's available for copying and what is not.
- Describe what's available on your site, and your organization. Be sure any general policies are clear.
- Keep information, especially READMEs, up-to-date. Provide READMEs in plain ascii text.
- Present a list of mirrors of your site if you know them. Make sure you include a statement of copyright applicable to your mirrors. List their update schedule if possible.
- Make sure that popular (and massive) information has the bandwidth to support it.

- Use conventions for file extensions - .txt for ascii text; .html or .htm for HTML; .ps for Postscript; .pdf for Portable Document Format; .sgml or .sgm for SGML; .exe for non-Unix executables, etc.
- For files being transferred, try to make filenames unique in the first eight characters.
- When providing information, make sure your site has something unique to offer. Avoid bringing up an information service which simply points to other services on the Internet.
- Don't point to other sites without asking first.
- Remember that setting up an information service is more than just design and implementation. It's also maintenance.
- Make sure your posted materials are appropriate for the supporting organization.
- Test applications with a variety of tools. Don't assume everything works if you've tested with only one client. Also, assume the low end of technology for clients and don't create applications which can only be used by Graphical User Interfaces.
- Have a consistent view of your information. Make sure the look and feel stays the same throughout your applications.
- Be sensitive to the longevity of your information. Be sure to date time-sensitive materials, and be vigilant about keeping this information well maintained.
- Export restrictions vary from country to country. Be sure you understand the implications of export restrictions when you post.
- Tell users what you plan to do with any information you collect, such as WWW feedback. You need to warn people if you plan to publish any of their statements, even passively by just making it available to other users.
- Make sure your policy on user information services, such as homepages, is well known.

Zdroj: [9].

Příloha č. 2:

Smilies (tzv. smajlíky)

Znaky	Význam
:-)	Smích
:-(	Zamračený, nešťastný, špatná nálada
:-|	Lhostejnost, žádný názor
:-r	Vystrčený jazyk
:-c	Opravdu nešťastný
:-<	Ztracený, opuštěný
:-7	Kyselý úsměv
:´-(	Plačící
:-D	Hlasitý smích
:-?	Uživatel kouří dýmku
8-)	Uživatel nosí brýle
:-[	Upír
:-p	Vypláznutý jazyk
(-:	Uživatel je levák
;-)	Smích s mrknutím oka, ironická poznámka
:->	Ďábelský úsměv, velmi sarkastická poznámka
:-V	Křik
:-#	Cenzurováno
:-C	Spadlá čelist, nevěřící
:-B	Plácající nesmysly
:~~)	Mít rýmu
:´-)	Plačící smíchy
:-/	Skeptický
:*)	Opilý
:-{)	Uživatel nosí knír
:^)	Natlučený nos
:-X	Zalepená ústa
%-)	Uživatel sedí u počítače už velice dlouho

Tab. 2: Smilies (smajlíky) a jejich význam; zdroj: [1].

Příloha č. 3:

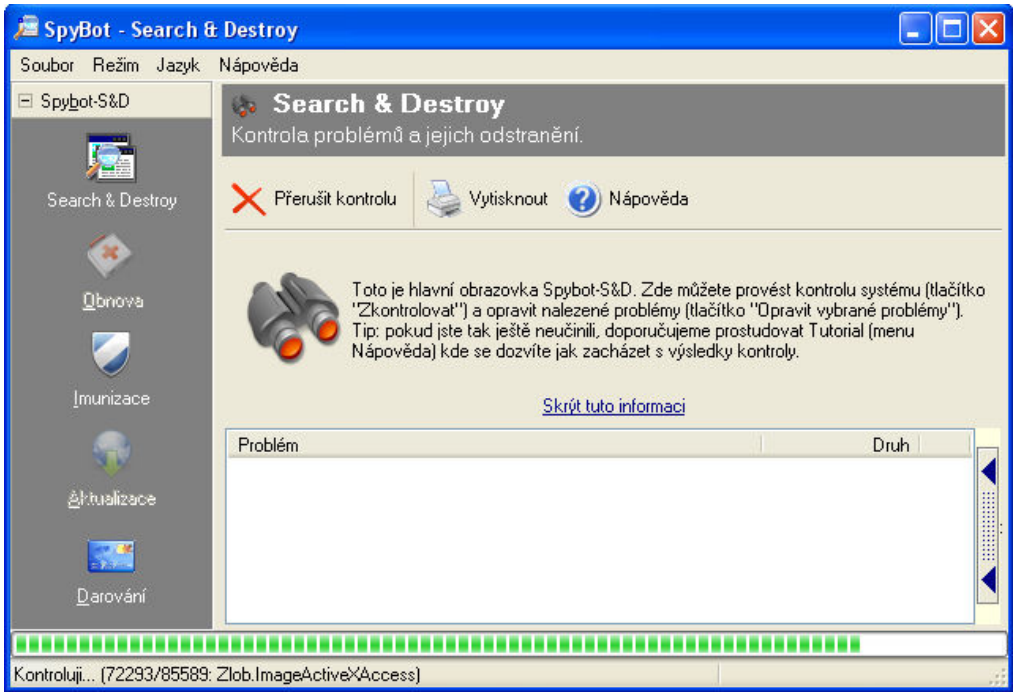
Program Ad-Aware SE Personal Edition (antispyware)

Obr. 2: Úvodní okno programu Ad-Aware SE; zdroj: vlastní.

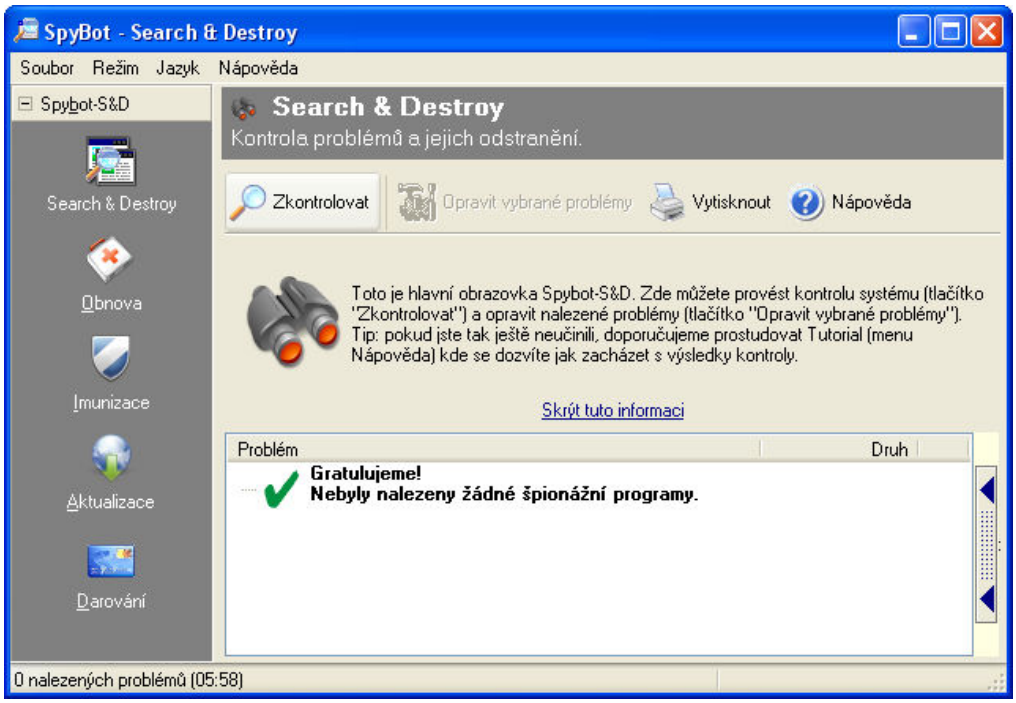
Obr. 3: Výsledky testu programu Ad-Aware SE; zdroj: vlastní.

Příloha č. 4:

Program Spybot – Search & Destroy (antispyware)



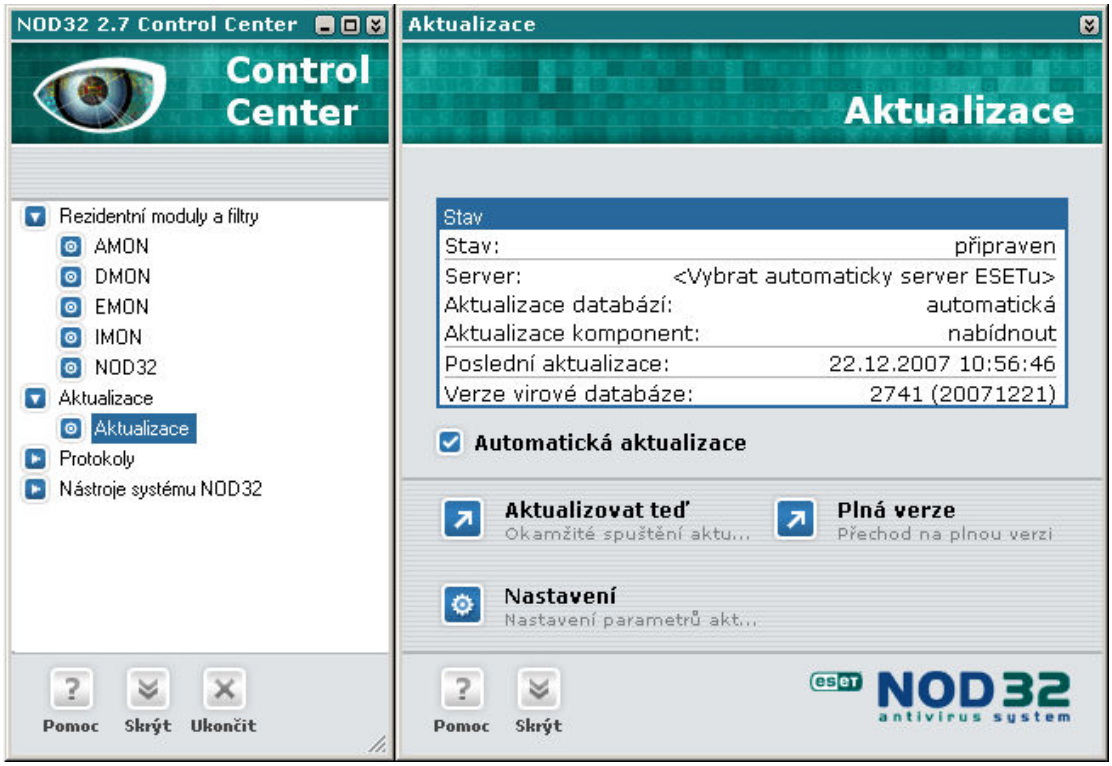
Obr. 4: Testování programem Spybot – Search & Destroy; zdroj: vlastní.



Obr. 5: Výsledky testování programem Spybot – Search & Destroy; zdroj: vlastní.

Příloha č. 5:

Antivirové programy

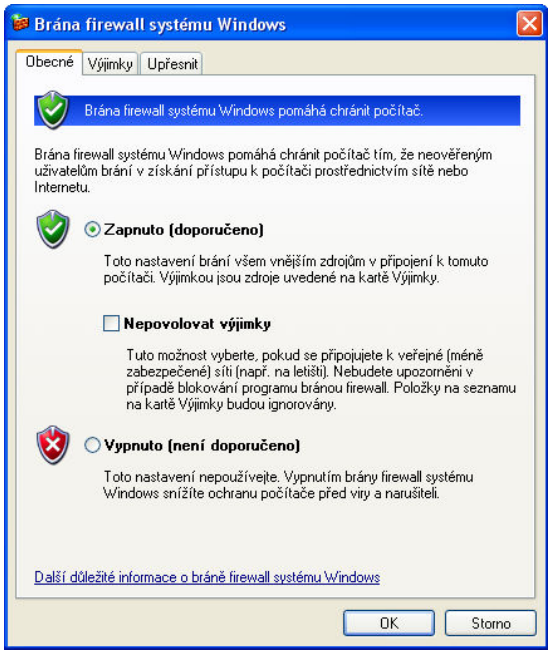


Obr. 6: Antivirový program NOD 32; zdroj: vlastní.

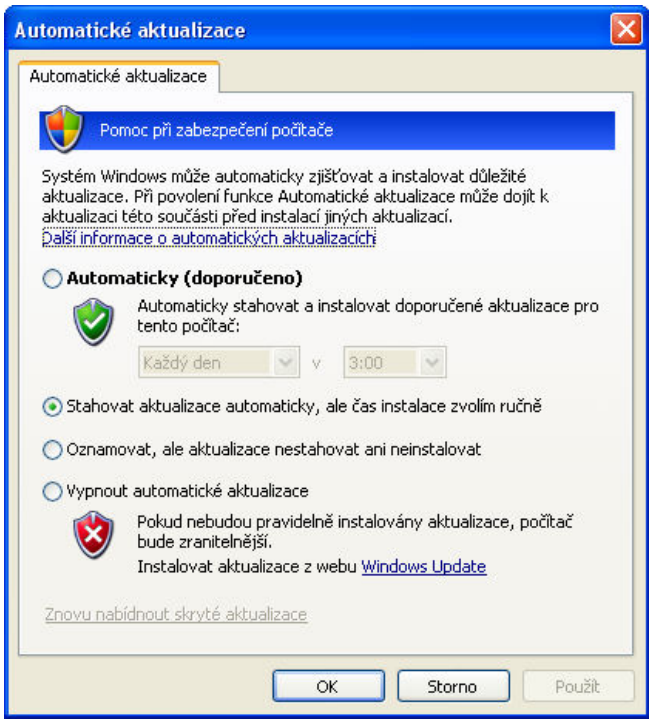
Obr. 7: Antivirový program avast!; zdroj: vlastní.

Příloha č. 6:

Firewall a automatické aktualizace systému Windows



Obr. 8: Okno nastavení brány firewall operačního systému Windows; zdroj: vlastní.



Obr. 9: Nastavení automatických aktualizací systému Windows; zdroj: vlastní.

Příloha č. 7:

Nejčastěji diskutované problémy týkající se autorského práva na Internetu

- Bez souhlasu autora nelze z Internetu převzít videoklipy, fotografie, zvukový soubor, nebo přetisknout texty písní, kreslený vtip, literární dílo a dále použít. Platí, i když autor není znám.
- Je nutné vždy zjišťovat, zda se jedná o autorské dílo, kdo je jeho autorem a získat jeho souhlas.
- Souhlas autora získat přímým kontaktováním. Není-li uveden, kontaktovat agenturu, nakladatelství, správce WWW stránek apod. V případě neúspěchu se dílo nedá použít.
- Lze přetisknout vyobrazení nějakého uměleckého díla. Není nutné autorův souhlas, pokud dílo převedl na jinou osobu (prodejem, darem aj.), vystavuje-li se dílo bezplatně či je-li k vystavení bezplatně půjčeno.
- Použitím určité literární postavy do vlastního díla lze, pokud osoba není nijak zvlášť specifická a jedinečná.
- Kopírovat design a obsah WWW stránek nelze. Vztahuje se i na skript, který WWW stránku tvoří.
- Zařazení odkazu na jinou stránku je legální. Na prostá zpravodajská oznámení se nevztahují autorská práva, protože se jedná o všeobecně známé informace (§ 34 písm. b) [24]. Pokud zpráva hodnotí a komentuje, je chráněna autorským právem. Další možností je převzetí článků zpřístupňujících zpravodajství o aktuálních věcech politických, hospodářských nebo náboženských, uveřejněné již v jiném hromadném sdělovacím prostředku. Dle § 31 [24] do práva autorského nezasahuje ten, kdo užije v odůvodněné míře výňatky ze zveřejněných děl jiných autorů ve svém díle, užije výňatky z díla nebo drobná celá díla pro účely kritiky nebo recenze vztahující se k takovému dílu, užije dílo při vyučování pro ilustrační účel nebo při vědeckém výzkumu. Vždy je nutno uvést jméno autora, je-li to možné.
- Dle občanského zákoníku lze použít pořízené fotografie nebo použít fotografie veřejně známých osob jen s jejich svolením. Bez svolení pouze ke zpravodajským účelům. Dle autorského zákona je důležité, kdo je autorem fotografie. Cizí fotografii lze zveřejnit pouze se souhlasem autora. Z toho vyplývá, že je nutné mít souhlas jak autora fotografie, tak fotografovaného. Výjimku tvoří dle § 37 odst. 2 písm. b) [24] zveřejnění své vlastní fotografie pořízené někým jiným.
- Otázka použití jména či loga nějaké společnosti je složitější. Jméno či logo může být chráněno obchodním jménem (dle obchodního zákoníku [17]) či ochrannou známkou (dle

zákona o ochranných známkách [28]). Bez souhlasu majitele ochranné známky nikdo nesmí jména či loga společnosti užít.

- Nelze přeložit dílo do jiného jazyka a zveřejnit bez souhlasu autora.
- Přes vlastní webové stránky lze distribuovat své vlastní produkty (např. programy) nebo umístit odkaz na volně stažitelné programy na cizích WWW stránkách. V žádném případě nelze distribuovat cizí díla na svých WWW stránkách.
- Vytvářet CD se soubory (hudba, texty, obrázky) staženými z Internetu lze, pokud jsou učeny pro vlastní potřebu. Neplatí pro počítačové programy a elektronické databáze.
- Půjčování, prodej či darování takových CD je nelegální.

Zdroj: [2].